International Journal of Computing Sciences Research (ISSN print: 2546-0552; ISSN online: 2546-115X)
Vol. 8, pp. 2995-3009
doi: 10.25147/ijcsr.2017.001.1.199
https://stepacademic.net

Short Paper

Balancing Usability and Security in Secure System Design: A Comprehensive Study on Principles, Implementation, and Impact on Usability

Taofeek O. Agboola
Department of Computer Science, Stephen F. Austin State University, United States of America
omoaweonline@gmail.com
agboolato@jacks.sfasu.edu
ORCID: 0009-0009-2882-7230
(corresponding author)

Job Adegede
Department of Computer Science, Stephen F. Austin State University, United States of America
adegedejo@jacks.sfasu.edu

John G. Jacob
Department of Informatics, Fort Hays State University, United States of America
jjjohnnybrag@gmail.com

Recommended citation:

Agboola, T. O., Adegede, J., & Jacob, J. G. (2024). Balancing usability and security in secure system design: a comprehensive study on principles, implementation, and impact on usability. *International Journal of Computing Sciences Research*, *8*, 2995-3009. https://doi.org/10.25147/ijcsr.2017.001.1.199

Abstract

Purpose - The purpose of this study is to provide a comprehensive analysis of the principles and implementation strategies of secure system design, emphasizing the critical balance between security and usability. This study aims to uncover how usability impacts the effectiveness of secure systems, exploring the human-centric approach to security. This research offers insights for organizations to develop systems that ensure robust security while providing a seamless, intuitive user experience.

Method - This study employs an extensive review of existing literature on secure system design principles, usability studies, and human-centric security approaches.

Result - Identification of fundamental principles that underpin secure system design, like confidentiality, integrity, availability, authentication, and authorization. Highlights common usability challenge, including complex authentication processes, poor interface design, and lack of user-friendly features. Examining the necessary trade-offs and providing strategies to achieve a balance between robust security measures and user convenience.

Conclusion – The study concludes that secure system design must adopt a human-centric approach, emphasizing usability's role in effective security. Technical measures are vital, but user behavior significantly impacts overall security. Addressing usability challenges enhances compliance and reduces risks. Integrating security and usability principles is essential for developing secure, user-friendly systems

Recommendation – Future research should focus on user-centered design for secure systems, incorporating continuous usability testing to promptly address issues. Provide comprehensive user education to enhance security awareness. Encourage collaboration between designers and security experts to create solutions that balance security and usability effectively.

Research Implication - The research highlights the critical link between usability and security in system design, underscoring the need for a human-centric approach. It provides guidelines for creating secure, user-friendly systems to boost compliance and reduce risks, while also informing policy and encouraging further exploration of balancing security and usability in technology.

Keywords – designing secure systems, sensitive data, usability impact

INTRODUCTION

The importance of designing secure systems has become increasingly crucial in light of the growing threats posed by cyberattacks. In today's interconnected digital world, the need for secure systems has never been greater. As technology continues to advance, so do the threats posed by cyberattacks, making it paramount to prioritize security in the design and implementation of systems. In this comprehensive study, we will delve into the principles, strategies, and best practices for designing secure systems.

Furthermore, we will explore the impact of security measures on usability, aiming to strike a balance between robust protection and user accessibility. Through this study, we seek to highlight the critical role of secure system design in safeguarding sensitive data and mitigating potential threats (Ferreira et al., 2009; Lin et al., 2015; Fiondella et al., 2016; Dong et al., 2018; Manson & Anderson, 2019; Lu et al., 2020, 2022; Mantha et al., 2021).

According to Mantha et al. (2021), by examining different methodologies and approaches, we can gain a better understanding of how to ensure the security of our systems while still maintaining usability. This study aims to provide a comprehensive examination of secure system design principles, implementation strategies, and their impact on usability. Furthermore, the study will explore the challenges and complexities involved in balancing security and usability, as well as identify potential conflicts and propose solutions (Beach et al., 2022). This study will not only provide insights into the current state of secure system design but also propose new approaches and methodologies to address emerging threats.

The study will also examine the impact of different security measures on usability, aiming to find a balance between robust protection and user-friendly experience. From the analysis of various sources, it is evident that designing secure systems involves a comprehensive understanding of security principles and the careful selection and implementation of appropriate controls to mitigate potential risks (Naqvi, Porras, Oyedeji, & Ullah, 2020; Beach et al., 2022; Jøsang et al., 2007). It is important to consider usability in the development of security systems to prevent user mistakes that could compromise the system's security. By incorporating security usability principles into the design and engineering process, developers can ensure that security solutions are not only effective against cyberattacks but also user-friendly. To achieve a successful balance between usability and security, it is necessary to establish patterns and principles that align both aspects from the start of the system development life cycle. This approach will help address potential conflicts between usability and security, allowing for the development of systems that are both secure and easy to use (Koupaei & Nazarov, 2020).

By incorporating security usability principles into the design and engineering process, developers can ensure that security solutions are not only effective against cyberattacks but also user-friendly (Jøsang et al., 2007). This approach will help minimize user mistakes and prevent compromises in security, ultimately leading to a more robust and user-friendly system. Furthermore, the study will explore the challenges and complexities involved in balancing security and usability, as well as identify potential conflicts and propose solutions (Naqvi, Porras, Oyedeji, & Ullah, 2020).

Methods for Designing Secure Systems

When looking at the methods for designing secure systems, it's essential to consider various approaches and best practices. One such approach is the principle of least privilege, which restricts users and programs to only the access they need to perform their tasks, thus minimizing potential damage from cyberattacks. Additionally, implementing strong encryption mechanisms, secure authentication protocols, and intrusion detection systems are crucial components of a comprehensive security strategy.

Balancing Security and Usability

Balancing security and usability is a complex task, as both aspects often seem to be at odds with each other. However, by integrating security into the early stages of system development and considering user behavior and needs, it is possible to create systems that are secure without sacrificing usability. This involves thoughtful user interface design, clear communication of security measures, and the implementation of user-friendly security features, such as biometric authentication or single sign-on systems (Cranor & Buchler, 2014; Realpe-Muñoz et al., 2017) The adoption of a user-centered design approach can greatly contribute to achieving this balance between security and usability (Jøsang et al., 2007).

The Role of Design Patterns

The role of design patterns in handling security and usability conflicts is crucial. Design patterns provide standardized solutions for common design problems, allowing developers to address both security and usability concerns effectively (Naqvi, Clarke, & Porras, 2020). By utilizing design patterns, developers can streamline the process of incorporating security and usability into their systems (Jøsang et al., 2007; Fiondella et al., 2016; Naqvi et al., 2020). This can lead to more efficient and effective security solutions that are also user-friendly (Naqvi, Porras, Oyedeji, & Ullah, 2020).

Ultimately, the goal is to create systems that prioritize both security and usability, ensuring that users can access their personal information safely while also experiencing a seamless and intuitive user interface (Modeling and analysis of security trade-offs - A goal-oriented approach, 2009). By considering usability from the beginning of the system development life cycle and incorporating design patterns that align security and usability, developers can create systems that are not only secure against attacks but also user-friendly (Realpe-Muñoz et al., 2017; Dalai & Jena, 2011).

Emerging Threats and Solutions

In today's evolving technological landscape, emerging threats continuously challenge the security of systems. Therefore, it is crucial to stay ahead of these threats by implementing proactive security measures and innovative solutions (Bayuk & Horowitz, 2011). These may include artificial intelligence-based security systems, blockchain technology for data integrity, and continuous monitoring and analysis of system behavior to detect anomalies and potential breaches. With these methods and considerations in mind, designing secure systems can effectively mitigate potential risks while maintaining a user-friendly experience (Elahi & Yu, 2009)

Understanding the Nature of Emerging Threats

Understanding the nature of emerging threats is essential in developing effective security measures. Researchers and developers must constantly stay informed about the latest trends in cyberattacks, vulnerabilities, and hacker techniques.

Emerging threats in the digital landscape are dynamic and ever-evolving. Cyber attackers are constantly finding new vulnerabilities and methods to exploit systems, posing a significant challenge to the security of digital infrastructures (Ross et al., 2021). It is essential to understand the nature of these emerging threats to effectively design and implement secure systems that can withstand and mitigate these risks.

Proactive Security Measures

In response to the evolving threat landscape, proactive security measures are essential to ensure the resilience of systems. Implementing artificial intelligence-based security systems can significantly enhance threat detection and response capabilities (Security by Design Principles - OWASP, 2016). By leveraging machine learning algorithms, these systems can adapt and evolve to identify and respond to new and complex threats in real-time, making them invaluable in safeguarding sensitive data and system integrity (Ahmadjee et al., 2022).

Moreover, the use of blockchain technology can enhance the security and integrity of data by providing an immutable ledger that records all transactions (Brunet & Mattavelli, 2023)

BLOCKCHAIN TECHNOLOGY FOR DATA INTEGRITY

As data integrity becomes an increasingly critical concern, blockchain technology offers a promising solution. By leveraging blockchain technology, systems can ensure the immutability and transparency of data, making it highly resistant to tampering or unauthorized modifications. Additionally, the decentralized nature of blockchain ensures that there is no single point of failure, making it more resilient against attacks (Rawat et al., 2020)

Blockchain technology offers a promising solution for maintaining the integrity of data within systems (Ahmadjee et al., 2022). Through its decentralized and tamper-evident nature, blockchain provides a secure and transparent method for recording and verifying digital transactions (Brunet & Mattavelli, 2023). Integrating blockchain technology into system design can ensure the authenticity and immutability of critical data, thereby enhancing security and trustworthiness.

Continuous Monitoring and Analysis of System Behavior

Another crucial aspect of designing secure systems is implementing continuous monitoring and analysis of system behavior (Zhang et al., 2020). This allows for the

detection of any abnormal activities or deviations from expected behavior, which could indicate a potential security breach or unauthorized access. By constantly monitoring and analyzing system behavior, organizations can quickly identify and respond to potential threats, minimizing the impact of cyberattacks (Elahi & Yu, 2009).

Continuous Monitoring and Analysis

Continuous monitoring and analysis of system behavior are crucial components of an effective security strategy (Naqvi et al., 2020). By leveraging advanced monitoring tools and analytics, organizations can detect anomalies, suspicious activities, and potential breaches in real-time. This proactive approach allows for immediate response and mitigation of security threats, bolstering the overall resilience of the system (Shirtz et al., 2024). To understand the nature of emerging threats and implement proactive security measures, organizations can effectively design and implement secure systems that mitigate potential risks while maintaining a user-friendly experience (Suhail & Jurdak, 2021). The incorporation of artificial intelligence-based security systems, blockchain technology, and continuous monitoring and analysis serves as a proactive defense against the ever-evolving landscape of cyber threats (Naik et al., 2021). Subsequently, the continuous growth in cyber threats necessitates the use of AI technology for quick and automatic responses to security attacks.

The Role of Artificial Intelligence in Cybersecurity

Artificial Intelligence plays a crucial role in modern cybersecurity efforts. By leveraging AI technology, organizations can enhance their ability to detect and respond to security threats in real-time (Chakraborty et al., 2022). AI-based security systems can analyze vast amounts of data from diverse sources, identify patterns indicative of potential security breaches, and autonomously initiate responsive actions. This proactive approach to threat detection and mitigation is essential in addressing the ever-evolving tactics of cyber attackers (Cadzow, 2019).

Artificial Intelligence has the potential to revolutionize cybersecurity by enabling predictive analysis, automating incident response, and continuously learning from new threats. (Naqvi et al., 2020) This evolution of technology has led to the development of advanced analytics, machine learning, and AI techniques in cybersecurity (Poddar, 2022; Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation, 2022). These advancements in AI technology are crucial for improving cybersecurity solutions and staying ahead of cybercriminals (University, 2023)

One of the key advantages of AI in cybersecurity is its ability to adapt and learn from new information (Securing the Future of AI and ML at Microsoft, 2022). Machine learning algorithms, a subset of AI, can continuously refine their understanding of normal and abnormal system behavior, enabling them to detect emerging threats and zero-day exploits (Artificial Intelligence in Cyber Security, 2023). By leveraging historical data and

behavior patterns, these algorithms can identify deviations that may indicate a security threat, thus strengthening the overall resilience of the system (Iannucci et al., 2020) to potential attacks.

Autonomous Response and Adaptive Defense

Another important aspect of AI in cybersecurity is its ability to autonomously respond to security threats and adapt its defense mechanisms. AI systems can analyze and prioritize threats, making quick decisions on how to respond based on predefined rules and algorithms. These systems can automatically implement remediation measures, isolate compromised components, and even dynamically adjust security protocols to counter ongoing attacks (Chiasson et al., 2007) This autonomous and adaptive nature of AI in cybersecurity significantly reduces the response time to security incidents, minimizing potential damage and mitigating the impact of attacks (Hoffman, 2021). AI-based security systems can also autonomously respond to new and evolving threats by dynamically adjusting their defense strategies based on real-time data analysis. This adaptability is crucial in the face of constantly changing attack techniques and tactics employed by cybercriminals (Goodwin & Caceres, 2022).

ETHICAL CONSIDERATIONS IN AI-BASED SECURITY SYSTEMS

The use of AI in cybersecurity also raises important ethical considerations. As AI becomes more prevalent in cybersecurity, it is essential to carefully consider the ethical implications of its use (Gupta, 2021). Some ethical considerations in AI-based security systems include: - Privacy concerns: AI systems often rely on large amounts of data to effectively detect and respond to threats. Privacy concerns arise regarding the collection, storage, and usage of personal and sensitive information.

i. Bias and discrimination: AI algorithms can inadvertently perpetuate biases present in the data they are trained on. This can result in discriminatory outcomes and unfair treatment of certain individuals or groups (Lu et al., 2020).
ii. Accountability and transparency: AI systems in cybersecurity may make autonomous decisions that can have significant consequences. It is crucial to establish clear lines of accountability and ensure transparency in the decision-making processes of AI-based security systems (Alshamari, 2016).
iii. Human oversight: While AI systems can automate certain aspects of cybersecurity, it is important to maintain human oversight and involvement in decision-making processes (Evtimov et al., 2020).

While the use of AI in cybersecurity offers significant advantages, it is essential to address the ethical considerations associated with its deployment. AI systems are only as effective as the data they are trained on, and biases within the training data can lead to discriminatory outcomes (Hintersdorf et al., 2023). Therefore, organizations must prioritize transparency and fairness in the development and implementation of AI-based

security systems (Evtimov et al., 2020). Ethical considerations also extend to the potential impact of AI on the workforce, as automation of certain security tasks may raise concerns about job displacement and the need for retraining employees (Sarker et al., 2023).

Collaboration Between Humans and AI

In addressing these ethical concerns, a collaborative approach that integrates human expertise with AI capabilities is paramount. While AI can analyze and process vast amounts of data at unprecedented speeds, human intuition, and ethical judgment are indispensable in interpreting complex situations and making decisions based on broader contextual understanding (Huang & Zhu, 2023).

The Future of AI in Cybersecurity

As AI technology continues to advance, the future of cybersecurity will likely see further integration of AI-driven capabilities (Sarker et al., 2023). Predictive analytics and preemptive threat intelligence, enabled by AI, will empower organizations to anticipate and prepare for potential threats, enhancing their overall resilience (Sarker et al., 2023). Additionally, AI's role in enabling faster incident response and recovery through automation and real-time decision-making is set to become increasingly pivotal in mitigating the impact of cyberattacks (Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects - Annals of Data Science, 2022).

In conclusion, the use of AI in cybersecurity represents a paradigm shift in the way organizations approach threat detection, response, and mitigation (Hoffman, 2021). By addressing the ethical considerations and leveraging the collaborative potential of humans and AI, organizations can harness the full capabilities of AI technology while ensuring responsible and effective cybersecurity practices. As the digital landscape continues to evolve, embracing AI as a central component of cybersecurity strategies will be crucial in staying ahead of ever-evolving cyber threats (Huang & Zhu, 2023).

Practical Implication of Balancing Usability and Security in Secure System Design

As technology continues to evolve, the need for secure systems that can effectively protect sensitive information has become increasingly crucial. However, designing such systems presents a delicate balance between ensuring robust security measures and maintaining a user-friendly experience (Salagrama, 2021). This paper explores the practical implications of this balance, examining the tradeoffs and considerations that must be made to create secure systems that are both effective and accessible.

One of the primary challenges in secure system design is addressing the root causes of software vulnerabilities, which can stem from both technical and user-side factors (Asadoorian et al., 2020). Technical vulnerabilities may arise from design flaws, coding errors, or inadequate testing, while user-side vulnerabilities can be attributed to improper practices, lack of awareness, or resistance to security measures. As security experts strive to mitigate these vulnerabilities, they must also consider the impact of their solutions on the user experience (Xu et al., 2022).

Overly restrictive security measures can hinder employee productivity and lead to workarounds that compromise security altogether. As Mitnick and Simon note, "Computer security is a balance between protecting information and enabling authorized access." Striking this balance requires a comprehensive understanding of user needs and behaviors, as well as the ability to design security controls that are both effective and unobtrusive (Thompson et al., 2020).

Research has shown that users often perceive security measures as impediments to their work, leading them to find ways to circumvent these controls. This underscores the importance of user-centered design in secure system development, where the needs and pain points of the end-user are carefully considered (Oliveira et al., 2018). As noted by Braz and Robert, "a system that's more secure is more predictable, more reliable, and hence more usable." This principle highlights the inherent synergy between usability and security, where the two goals can often be aligned rather than at odds (Cranor & Buchler, 2014).

By incorporating user feedback and understanding their needs, designers can create security measures that are intuitive, efficient, and seamlessly integrated into the user experience. This may involve streamlining authentication processes, minimizing the number of security-related tasks, or providing clear guidance on secure practices (Niroop, 2024). Additionally, educating users on the importance of security and helping them develop good digital hygiene can foster a culture of security awareness, reducing the likelihood of user-side vulnerabilities.

Balancing usability and security is not a one-size-fits-all solution, as the specific requirements and constraints of each system can vary greatly(Post & Kagan, 2007). Designers must carefully analyze the trade-offs, weigh the risks, and make informed decisions that prioritize both security and user experience(Faily et al., 2015). Ongoing user testing, iterative design, and a willingness to adapt to changing needs can help organizations strike this delicate balance and create secure systems that are both effective and user-friendly.

CONCLUSION

In conclusion, the continued integration of AI in cybersecurity represents a paradigm shift in the way organizations approach threat detection, response, and

mitigation. The combination of AI's computational power with human expertise and ethical judgment is crucial in addressing the complex and evolving landscape of cyber threats. By embracing a balanced approach that leverages the collaborative potential of humans and AI, organizations can effectively harness the full capabilities of AI technology while ensuring responsible and effective cybersecurity practices. As the digital landscape continues to evolve with increasingly sophisticated cyber threats, the successful deployment of AI in cybersecurity measures necessitates an in-depth understanding of its capabilities, challenges, and ethical implications. It is essential for organizations to continually adapt and improve their cybersecurity measures by incorporating AI systems that can proactively discover vulnerabilities, detect anomalies, and predict potential threats, as well as human experts who can provide contextual understanding and critical thinking in addressing security challenges. Looking ahead, the future of AI in cybersecurity will rely on the seamless integration of AI-driven capabilities and human expertise to enhance organizations' overall resilience against cyber threats. By addressing ethical considerations and leveraging the collaborative potential of human-AI teaming, organizations can establish trust in AI-driven security solutions and improve their overall cyber defenses. In today's rapidly changing world, the significance of accurate weather forecasts cannot be overstated. As we move towards the future, it is essential to recognize the potential of AI technologies in improving cybersecurity measures. As we move toward the future, it is essential to recognize the potential of AI technologies in improving cybersecurity measures and staying ahead of evolving threats. In today's rapidly changing world, the continued integration of AI in cybersecurity represents a paradigm shift in the way organizations approach threat detection, response, and mitigation.

ACKNOWLEDGMENT

To our course advisors, Dr. Zheng Jianjun, and our institution, Stephen F. Austin State University, for creating the enabling environment for us to carry out this research, we express our gratitude. We also thank our friends, relatives, and family who supported us morally, financially, or physically in various ways.

FUNDING

This research received no specific grant from any funding institution in the public, commercial, or not-for-profit sectors.

DECLARATION

Conflict of Interest

The author declared that there is no conflict of interest.

Inform Consent

This may not be applicable because this is a review article, and respondents are not involved.

Ethics Approval

It is not applicable because this is a review article, and no respondents are required.

REFERENCES

Ahmadjee, S., Mera-Gómez, C., Bahsoon, R., & Kazman, R. (2022). A Study on Blockchain Architecture Design Decisions and Their Security Attacks and Threats. *ACM Transactions on Software Engineering and Methodology, 31*(2), 1-45. https://doi.org/10.1145/3502740

Alshamari, M. (2016). A Review of Gaps between Usability and Security/Privacy. *International Journal of Communications, Network and System Sciences, 09*(10), 413-429. https://doi.org/10.4236/ijcns.2016.910034

Asadoorian, A., Alberto, M., & Ali, M. L. (2020, October). Creating and using secure software. In *2020 11th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0786-0792). IEEE.

Bayuk, J L., & Horowitz, B M. (2011). An architectural system engineering methodology for addressing cyber security. *Systems Engineering, 14*(3), 294-304. https://doi.org/10.1002/sys.20182

Beach, P. M., Mailloux, L. O., Langhals, B. T., & Mills, R. F. (2022). Analysis of systems security engineering design principles for the development of secure and resilient systems. In *Handbook of Scholarly Publications from the Air Force Institute of Technology (AFIT), Volume 1, 2000-2020* (pp. 33-63). CRC Press. https://doi.org/10.1109/access.2019.2930718

Brunet, S C., & Mattavelli, M. (2023, September 29). Secure-by-design smart contract based on dataflow implementations. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2309.17200

Cadzow, A. (2019, June 10). *Balancing functionality, usability, and security in design*. https://blog.c3l-security.com/2019/06/balancing-functionality-usability-and.html

Chakraborty, A., Biswas, A., & Khan, A K. (2022, September 27). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. *arXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2209.13454

Chiasson, S., Biddle, R., & Somayaji, A. (2007, January 1). Even Experts Deserve Usable Security: Design guidelines for security management systems. https://www.semanticscholar.org/paper/Even-Experts-Deserve-Usable-Security%3A-Design-for-Chiasson-Biddle/106993f734c41155873d7a9873755a3413d4ba1a

Cranor, L F., & Buchler, N. (2014). Better Together: Usability and Security Go Hand in Hand. *IEEE Security & Privacy, 12*(6), 89-93. https://doi.org/10.1109/msp.2014.109

Dalai, A. K., & Jena, S. K. (2011, February). Evaluation of web application security risks and secure design patterns. In *Proceedings of the 2011 International Conference on Communication, Computing & Security* (pp. 565-568). ACM. https://doi.org/10.1145/1947940.1948057

Dong, N., Zhao, J., Liu, Y., & Kong, Y. (2018). Research on Information Security System of Smart City Based on Information Security Requirements. *Journal of Physics: Conference Series, 1069*, 012040-012040. https://doi.org/10.1088/1742-6596/1069/1/012040

Elahi, G., & Yu, E. (2009). Modeling and analysis of security trade-offs–A goal-oriented approach. *Data & Knowledge Engineering*, *68*(7), 579-598.

Evtimov, I., Cui, W., Kamar, E., Kıcıman, E., Kohno, T., & Li, J. (2020, July 13). Security and Machine Learning in the Real World. *arXiv preprint*. https://doi.org/10.48550/arxiv.2007.07205

Faily, S., Lyle, J., Fléchais, I., & Simpson, A. (2015). *Usability and Security by Design: A Case Study in Research and Development.* Internet Society. https://doi.org/10.14722/usec.2015.23012

Ferreira, A., Rusu, C., & Roncagliolo, S. (2009, February). Usability and security patterns. In *2009 Second International Conferences on Advances in Computer-Human Interactions* (pp. 301-305). IEEE. https://doi.org/10.1109/achi.2009.21

Fiondella, L., Nikora, A., & Wandji, T. (2016, October). Software reliability and security: challenges and crosscutting themes. In *2016 IEEE International Symposium on Software Reliability Engineering Workshops (ISSREW)* (pp. 55-56). IEEE. https://doi.org/10.1109/issrew.2016.47

Goodwin, V H., & Caceres, R S. (2022, April 19). System Analysis for Responsible Design of Modern AI/ML Systems. *arXiv preprint.* https://doi.org/10.48550/arxiv.2204.08836

Gupta, A. (2021, January 28). Making Responsible AI the Norm rather than the Exception. *arXiv preprint*. https://doi.org/10.48550/arxiv.2101.11832

Hintersdorf, D., Struppek, L., & Kersting, K. (2023, August 18). Balancing Transparency and Risk: The Security and Privacy Risks of Open-Source Machine Learning Models. *arXiv preprint*. https://doi.org/10.48550/arxiv.2308.09490

Hoffman, W. (2021). Making AI Work for Cyber Defense. *Center for Security and Emerging Technology*. https://doi.org/10.51593/2021ca007

Huang, L., & Zhu, Q. (2023, January 14). An Introduction of System-Scientific Approaches to Cognitive Security. *arXiv preprint*. https://doi.org/10.48550/arxiv.2301.05920

Iannucci, S., Abdelwahed, S., Montemaggio, A., Hannis, M., Leonard, L., King, J., & Hamilton, J A. (2020). A Model-Integrated Approach to Designing Self-Protecting Systems. *IEEE Transactions on Software Engineering,* 46(12), 1380-1392. https://doi.org/10.1109/tse.2018.2880218

Jøsang, A., AlFayyadh, B., Grandison, T., AlZomai, M., & McNamara, J. (2007, December). Security usability principles for vulnerability analysis and risk assessment. In *Twenty-*

Third Annual Computer Security Applications Conference (ACSAC 2007) (pp. 269-278). IEEE. https://doi.org/10.1109/acsac.2007.14

Koupaei, A. N. A., & Nazarov, A. N. (2020, November). A hybrid security solution for mitigating cyber-attacks on info-communication systems. In *2020 International Conference Engineering and Telecommunication (En&T)* (pp. 1-4). IEEE. https://doi.org/10.1109/ent50437.2020.9431296

Lin, C., Zheng, B., Zhu, Q., & Sangiovanni-Vincentelli, A. (2015, December 2). Security-Aware Design Methodology and Optimization for Automotive Systems. *ACM Transactions on Design Automation of Electronic Systems, 21*(1), 1-26. https://doi.org/10.1145/2803174

Lu, Q., Zhu, L., Xu, X., & Whittle, J. (2022, March 2). Responsible-AI-by-Design: a Pattern Collection for Designing Responsible AI Systems. *arXiv preprint*. https://doi.org/10.48550/arxiv.2203.00905

Lu, Y. F., Kuo, C. F., Chen, H. M., Tseng, H. W., Chou, S. C., & Liao, Y. M. (2020, October). A Three-Factor Mutual Authentication Scheme for Cyber-Physical Systems. In *Proceedings of the International Conference on Research in Adaptive and Convergent Systems* (pp. 113-118). ACM. https://doi.org/10.1145/3400286.3418236

Manson, S., & Anderson, D. (2019, July 1). Cybersecurity for Protection and Control Systems: An Overview of Proven Design Solutions. *IEEE Industry Applications Magazine, 25*(4), 14-23. https://doi.org/10.1109/mias.2018.2875175

Mantha, B R K., Soto, B G D., & Karri, R. (2021, March 1). Cyber security threat modeling in the AEC industry: An example for the commissioning of the built environment. *Sustainable Cities and Society, 66*, Article 102682. https://doi.org/10.1016/j.scs.2020.102682

Naik, B B., Mehta, A., Yagnik, H., & Shah, M. (2021). The impacts of artificial intelligence techniques in augmentation of cybersecurity: a comprehensive review. *Complex & Intelligent Systems, 8*(2), 1763-1780. https://doi.org/10.1007/s40747-021-00494-8

Naqvi, B., Clarke, N., & Porras, J. (2020, August 12). Incorporating the human facet of security in developing systems and services. *Information & Computer Security, 29*(1), 49-72. https://doi.org/10.1108/ics-11-2019-0130

Naqvi, B., Porras, J., Oyedeji, S. & Ullah, M. (2020). Aligning security, usability, user experience: A pattern approach. In: Loizides, F., Winckler, M., Chatterjee, U., Abdelnour-Nocera, J. and Parmaxi, A. (eds.) *Human-Computer Interaction and Emerging Technologies: Adjunct Proceedings from the INTERACT 2019 Workshops* (pp. 267–278). Cardiff: Cardiff University Press. https://doi.org/10.18573/ book3.aj. https://doi.org/10.18573/book3.aj

Niroop, S. (2024, March 9). Contemplating Secure and Optimal Design Practices for Information Infrastructure from a Human Factors Perspective. *arXiv preprint.* https://arxiv.org/abs/2403.07018

Poddar, H. (2022, July 3). *An assessment of artificial intelligence in the cybersecurity sector*. Retrieved from https://pub.towardsai.net/an-assessment-of-artificial-intelligence-in-the-cybersecurity-sector

Post, G. V., & Kagan, A. (2007). Evaluating information security tradeoffs: Restricting access can interfere with user tasks. *Computers & Security*, *26*(3), 229-237. https://doi.org/10.1016/j.cose.2006.10.004

Rawat, B. D., Chaudhary, V., & Doku, R. (2020). Blockchain technology: Emerging applications and use cases for secure and trustworthy smart systems. *Journal of Cybersecurity and Privacy*, *1*(1), 4-18. https://doi.org/10.3390/jcp1010002

Realpe-Muñoz, P., Collazos, C. A., Granollers, T., Muñoz-Arteaga, J., & Fernandez, E. B. (2017, September). Design process for usable security and authentication using a user-centered approach. In *Proceedings of the XVIII International Conference on Human-Computer Interaction* (pp. 1-8). ACM. https://doi.org/10.1145/3123818.3123838

Ross, R., Pillitteri, V., Graubart, R., Bodeau, D., & McQuaid, R. (2019). *Developing cyber resilient systems: a systems security engineering approach (No. NIST Special Publication (SP) 800-160 Vol. 2 (Draft))*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-160v2r1

Salagrama, S. (2021). An Effective Design of Model for Information Security Requirement Assessment. *International Journal of Advanced Computer Science and Applications*, *12*(10). https://doi.org/10.14569/ijacsa.2021.0121001

OWASP. (2016, August 3). *Security by design principles.* Retrieved from https://wiki.owasp.org/index.php/Security_by_Design_Principles

Shirtz, D., Koberman, I., Elyashar, A., Puzis, R., & Elovici, Y. (2024, February 18). Enhancing Energy Sector Resilience: Integrating Security by Design Principles. *arXiv preprint*. https://doi.org/10.48550/arxiv.2402.11543

Suhail, S., & Jurdak, R. (2021, May 18). Towards Trusted and Intelligent Cyber-Physical Systems: A Security-by-Design Approach. *arXiv preprint*. https://doi.org/10.48550/arxiv.2105.08886

Xu, D., Chen, T., Tan, Z., Wu, F., Gao, J., & Yang, Y. (2022). Web Vulnerability Detection Analyzer Based on Python. *International Journal of Digital Crime and Forensics (IJDCF)*, *14*(2), 1-17. https://doi.org/10.4018/ijdcf.302875

Thompson, A. F., Oyinloye, O. E., David, M. T., & Alese, B. K. (2020). A Secured System for Internet Enabled Host Devices. *Network and Communication Technologies*, *5*(1), 26-36. https://doi.org/10.5539/nct.v5n1p26

Zhang, J., Tang, L., & Yang, G. (2020, June). Design of Security Management and Control Platform for Business System. In *2020 IEEE 4th Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)* (Vol. 1, pp. 784-787). IEEE. https://doi.org/10.1109/itnec48623.2020.9084999

Author's Biography

Taofeek Agboola is an early career cybersecurity professional with a robust background in endpoint analysis, network security, and vulnerability assessments. He is adept at monitoring networks for security risks, implementing secure cloud configurations, and performing thorough incident responses. He holds a Master of Science in Cybersecurity from Stephen F. Austin State University and a Bachelor of Science in Computer Science from Adekunle Ajasin University. Taofeek is also certified in CompTIA Security+, $(ISC)^2$ Certified in Cybersecurity, and Cisco's Networking Essentials, among others. His professional affiliations include the International Information System Security Certification Consortium $(ISC)^2$ and the Association for Computing Machinery.

Job Adegede is a data network Infrastructure Architect with an MSc in Cybersecurity from Stephen F. Austin State University, TX, and an MSc in Global Management from the University of Salford, UK. He's an avid technology specialist and business process analyst with a domain specialization in data network security and performance management.

John G. Jacob is an accomplished Security & Compliance Analyst with over six years of professional experience in the field of cybersecurity. He holds a Master's degree in Cybersecurity from Fort Hays State University and a Bachelor's degree in Computer Science from Adekunle Ajasin University. John is certified in several key areas, including CompTIA Security+, A+, AZ500, and CySA+, showcasing his broad expertise and commitment to continuous learning.