Research Proposal – Transcript – Haseeb Abdulhak

My name is Haseeb Abdulhak, in this presentation, I discuss the research proposal for Research Methods and Professional Practice as a module in University of Essex. The project title is Investigating the specific security vulnerabilities related to the human factor in IoT systems in secondary education.

Problem Statement

The Verizon (2022) report shows that human influences are the primary driver of data breaches, with 82% of breaches involving human involvement, these breaches may result from misuse of login credentials, phishing scams, intentional system misuse, or mistakes. Moreover, according to global risk report, in 95% of all cybersecurity issues, human error emerged as a significant contributing factor (World Economic Forum, 2022).

The human factor is a major contributor to security vulnerabilities in IoT systems. This is because humans are often the weakest link in the security chain (Kadena & Gupi, 2021).

The implications of IoT device vulnerabilities in education can have serious consequences for educational institutions and their stakeholders. The following are some of the consequences: Privacy concerns, IoT devices contain sensors such as position, microphone, and camera that require access to the location, sound recording to receive commands and make calls, or recording video, as well as they may store personal information (Sikder et al., 2018). Compromising these devices can violate students' privacy and reveal sensitive data such as the location, record conversations and capture video.

Additionally, Cyberattacks on IoT devices can disrupt educational services by causing downtime and lost productivity for educational institutions, affecting online learning platforms, student information systems, and communication systems. The Mirai Botnet is widely regarded as one of the most perilous cyberattacks targeting IoT networks. Its ability to transform interconnected consumer devices into a botnet capable of executing Distributed Denial of Service (DDoS) attacks renders it particularly menacing (Ghorbani et al., 2018). The occurrence of such attacks may cause disruptions in the provision of services by educational institutions, thereby impacting the accessibility and availability of educational resources (Babu et al., 2019).

Moreover, cyberattacks can have a wide range of negative effects and severe consequences. Such threats may result in financial losses as well as harm to an organization's social standing and reputation (alhasan, 2023). Educational institutions may suffer financial losses because of cyberattack costs such as remediation, lost productivity, and legal fees (Yaacoub et al., 2023). Hackers prioritize financial gains and use them for illegal income and funding. According to the IBM Cost of Data Breach report (2022), critical infrastructure organizations experienced an average data breach cost of USD 4.82 million, including the education sector.

Significance

This research will contribute to the expanding body of knowledge on IoT security in education. The findings of the study may be of interest to anyone concerned in education, security, and policymaking. The findings of this study can be used to improve security measures for IoT devices in secondary education.

Research Question

What are the specific security vulnerabilities related to the human factor in IoT systems in secondary education?

Aims and Objectives

The fundamental aim of this study proposal is to investigate and comprehend the vulnerabilities caused by human and behaviour aspects in the context of IoT systems deployed in secondary school settings. This research's objectives are to identify the human and behaviour elements that contribute to IoT vulnerabilities in secondary education, assess their impact on security, and suggest measures for enhancement.

Key literature

Hughes-Lartey et al. (2021) conducted a study of data breach incidents in the healthcare sector that violated the US Health Information Privacy Protection Act (HIPA) from 2009 to 2017. While the study focuses on human factors causing breaches in the healthcare sector, it may overlook other significant factors such as poor security configuration and unpatched firmware/software, which can also lead to data breaches. For example, an IPv4 scan found 1.8 million vulnerable IoT devices because of misconfiguration or default configuration that could be used to launch large-scale attacks, these devices could be used to infect other

devices with malware or to launch distributed denial-of-service (DDoS) attacks (Srinivasa et al.,2021).

Additionally, the study also investigated the violations reported in America and regarding the health care sector and may not be representative of data breach incidents in other countries, in addition it may not apply to the secondary education sector.

Ataç & Akleylek (2019) discuss the vulnerability of common IoT devices due to weak computing power and a lack of security measures, and examine various threats faced by IoT systems, such as weak passwords, a lack of encryption, insecure updates, vulnerabilities in network protocols, and software/firmware flaws, as well as highlight prevalent attacks including DDoS, malware propagation, phishing, data theft, and device tampering resulting from widespread IoT adoption.

While the paper primarily focuses on technical aspects of IoT security, it does superficially discuss human errors as a category of vulnerabilities or threats in IoT systems. It does not provide an in-depth analysis of human factors, such as human errors, as specific vulnerabilities, or threats in IoT systems. However, it does acknowledge the potential impact of these techniques on IoT security.

Choudhary et al. (2021) explore the security concerns related to IoT systems, encompassing potential risks, vulnerabilities, and prospective solutions to enhance security. They pointed out vulnerabilities based on the Open Web Application Security Project (OWASP) IoT Top 10 2018. They argue that, despite the attacks, there has been no significant improvement in security. Long-term use of internet of things devices makes them more vulnerable over time, therefore it's crucial to have timely updates and patches (Choudhary et al.,2021).

However, there are a few limitations. According to Ferrara et al. (2021), the OWASP IoT Top 10 categories research reveals that IoT security flaws may be generally divided into three key areas: software, system, and device hardware. This means that it does not address other general security risks like phishing and social engineering. Another limitation is that the OWASP IoT Top 10 was released in 2018 and may not represent current and emerging IoT security risks and vulnerabilities.

Davis et al. (2022) assessed security vulnerabilities in various IoT devices. They conclude that the adoption of IoT devices has introduced security and privacy risks into the once-secure

personal environment. Interestingly, they observed that devices from less popular manufacturers have not been researched for vulnerabilities, indicating possible security weaknesses.

While the study provides useful documentation of vulnerabilities, it examines a case study of smart home IoT devices that may not be applicable to other types of IoT devices or environments. Therefore, further research is needed to assess the security risks and vulnerabilities of other types of IoT devices in secondary education environments.

A study by Zhao et al. (2020) analysed over 1.3 million IoT devices and found that 28.25% had at least one known vulnerability, primarily in authentication and authorization, such as weak passwords and default credentials. According to Zhao et al. (2020), misconfiguration is one of the most serious difficulties that IoT devices face today. This is because IoT devices are frequently misconfigured with default passwords or credentials, making them easier for attackers to exploit. They highlighted that, despite its extensive history, there are no signs of improvement. Vendors frequently fail to propose remedies for this important issue. This is supported by Polat & Sodah (2019). Although IoT devices have poor security and several weaknesses, manufacturers are not prioritizing improving the security of devices, and developers are still producing immature devices in terms of security (Polat & Sodah, 2019).

While there are valuable findings in the study, there are limitations to consider. The study may not capture the entire landscape of IoT device security, as it is limited to a specific sample size and six categories of devices such as security cameras, routers, smart home devices, DVRs, NAS devices, and printers. Additionally, the study does not examine IoT devices that are used in secondary schools, such as smart boards and sensors.

Methodology/Research Design

An exploratory approach that collects a large amount of data before making precise conclusions is appropriate for researching the human factor's special vulnerabilities in IoT systems in the context of education.

Mix method research, which combines both qualitative and quantitative approaches, will be used to gather and analyse data. With the quantitative method, we will conduct a content analysis of research papers, reports, and documents that include quantitative data on vulnerabilities, incidents, and breaches concerning the human factor in IoT system security.

With the quantitative method, we will compile and statistically analyse available quantitative sources, such as literature, surveys, and case studies, on IoT device security and incidents to identify correlations between human factors and vulnerabilities.

Hypothesis 1: Most vulnerabilities introduced into secondary school IoT environments originate from errors or mistakes by vendors and end users such as students and staff.

Hypothesis 2: Human factors risks in secondary school IoT systems originate from a lack of awareness of security best practices.

Ethical Considerations & Risk Assessment

Because this is secondary research that does not include direct engagement with individuals, ethical considerations are not a significant issue. However, it is critical to ensure that the data utilized in this study was gathered ethically and in accordance with applicable legislation and norms. Conduct the study in an objective and fair way, with no prejudice or preference toward certain vendors, technologies, or groups. When choosing, representing, and interpreting secondary sources, accuracy and objectivity are crucial to avoid distortion or misinterpretation.

In terms of risk assessment, secondary research should consider data from different sources that vary in quality and reliability. It is crucial to evaluate the data's quality and ensure that the findings are based on accurate and reliable information. Furthermore, the findings from the research may be specific to the context of IoT technology in secondary education and may not be generalizable to other sectors. It is important to consider the limitations of the research and the extent to which the findings can be applied to other contexts.

Artefacts

The research aims to create two artifacts. The first artifact is a comprehensive research report that includes a full examination of the unique IoT vulnerabilities in secondary education connected to human and behaviour aspects. The report will give a clear and organized summary of the findings based on a comprehensive study of academic sources and reports. The study report will give important insights into the existing state of IoT security in secondary education and highlight areas for development.

The second artifact is a best practice guide that provides clear, practical strategies and recommendations for improving IoT security in secondary education based on research findings. The guide will cover different aspects of IoT security, including user awareness, training, device management, and network security practices. It will be a valuable resource for end users such as educators, administrators, and IT professionals working in the secondary education sector, as well as for manufacturers and developers of IoT devices.

Timeline

The timeline of proposed activities for the project includes a literature review, data collection, data analysis, report writing, and review and submission. Seven months are scheduled for the completion of all project activities. One month for conducting a systematic literature review of academic research publications to examine industry reports, investigate past news reports and analyses of IoT-related incidents or data breaches, and examine publicly available IoT device information from manufacturers commonly used in schools. Two months are planned to conduct a content analysis of research papers, reports, and documents that include quantitative data on vulnerabilities, incidents, and breaches. Two months are planned to compile and statistically analyse the available quantitative sources of data. Then one month is planned for finding and outcome evaluation, and the final month is dedicated to generating a report, reviewing it, and submitting it.

Thank you.

References

Alhasan, Isslam Yousef (2023) Human Factors in Cybersecurity: A Cross-Cultural Study on Trust. *Purdue University Graduate School*. DOI: https://doi.org/10.25394/PGS.23271581.V1.

Ataç, C., & Akleylek, S. (2019) A Survey on Security Threats and Solutions in the Age of IoT. *European Journal of Science and Technology* : 36-42. DOI: https://doi.org/10.31590/ejosat.494066.

Babu, P. D., Pavani, C., & Naidu, C. E. (2019) Cyber security with IoT. *2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM)* 109–113. DOI: https://doi.org/10.1109/ICONSTEM.2019.8918782

Choudhary, Y., Umamaheswari, B., & Kumawat, V. (2021) A Study of Threats, Vulnerabilities and Countermeasures: An IoT Perspective. *Shanlax International Journal of Arts, Science and Humanities* 8(4): 39-45. DOI: https://doi.org/10.34293/sijash.v8i4.3583.

Davis, B. D., Mason, J. C., & Anwar, M. (2020) Vulnerability Studies and Security Postures of IoT Devices: A Smart Home Case Study. *IEEE Internet of Things Journal* 7(10): 10102–10110. DOI: https://doi.org/10.1109/JIOT.2020.2983983.

Ferrara, P., Mandal, A. K., Cortesi, A., & Spoto, F. (2021) Static analysis for discovering IoT vulnerabilities. *International Journal on Software Tools for Technology Transfer 23*(1): 71–88. DOI: https://doi.org/10.1007/s10009-020-00592-x

Ghorbani, H., Izadyar, M., Deilami, H. A., & Ahmadzadegan, M. H. (2018) Massive ddos occurrence investigation in future iot devices. *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)* 695–698. DOI: https://doi.org/10.1109/ISRITI.2018.8864445

Hughes-Lartey, K., Li, M., Botchey, F. E., & Qin, Z. (2021) Human factor, a critical weak point in the information security of an organization's Internet of things. *Heliyon* 7(3). DOI: https://doi.org/10.1016/j.heliyon.2021.e06522.

IBM (2022) Cost of a Data Breach Report 2022. Available from: https://www.key4biz.it/wp-content/uploads/2022/07/Cost-of-a-Data-Breach-Full-Report-2022.pdf [Accessed 13 August 2023].

Kadena, E., & Gupi, M. (2021) Human factors in cybersecurity: Risks and impacts. *Security Science Journal 2*(2): 51–64. DOI: https://doi.org/10.37458/ssj.2.2.3

Kolias, C., Kambourakis, G., Stavrou, A. & Voas, J. (2017) DDoS in the IoT: Mirai and Other Botnets. *Computer* 50(7): 80–84. DOI: https://doi.org/10.1109/mc.2017.201.

OWASP (2018) OWASP Internet of Things Project - OWASP. Available from: https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10 [Accessed 12 August 2023].

Polat, G. & Sodah, F. (2019) Security Issues in IoT: Challenges and Countermeasures. *ISACA*. Available from: https://www.isaca.org/resources/isaca-journal/issues/2019/volume-1/security-issues-in-iot-challenges-and-countermeasures [Accessed 15 August 2023].

Sikder, A., Petracca, G., Aksu, H., Jaeger, T., & Uluagac, A. (2018) A survey on sensor-based threats to internet-of-things (Iot) devices and applications. *ArXiv*. Available from: https://www.semanticscholar.org/paper/70335f9b6d0a76533dfd5255cc3a5e313e76a398 [Accessed 13 August 2022].

Srinivasa, S., Pedersen, J. M., & Vasilomanolakis, E. (2021) Open for hire: Attack trends and misconfiguration pitfalls of IoT devices. *Proceedings of the 21st ACM Internet Measurement Conference* 195–215. DOI: https://doi.org/10.1145/3487552.3487833

Verizon (2022) 2022 Data Breach Investigations Report. Available from: https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf [Accessed 9 August 2022].

World Economic Forum (2022) The Global Risks Report 2022. Available from: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf [Accessed 11 August 2023].

Yaacoub, J.-P. A., Noura, H. N., Salman, O., & Chehab, A. (2023) Ethical hacking for IoT: Security issues, challenges, solutions and recommendations. *Internet of Things and Cyber-Physical Systems 3*: 280–308. DOI: https://doi.org/10.1016/j.iotcps.2023.04.002

Zhao, B., Ji, S., Lee, W.-H., Lin, C., Weng, H., Wu, J., Zhou, P., Fang, L., & Beyah, R. (2022) A Large-Scale Empirical Study on the Vulnerability of Deployed IoT Devices. *IEEE Transactions on Dependable and Secure Computing* 19(3):1826-1840. DOI: https://doi.org/10.1109/TDSC.2020.3037908.