Information Security and Risk Assessment associated with meeting modes

By

M.M.A.S.T. Akmeemana - Index No: 20020015
A.I. Vidanage - Index No: 20021089
K.P.G.K. Jayathilake - Index No: 20020521

Supervisor: Dr. C.I. Kappetiyagama

Co-supervisor: Mr. Tharindu Wijethilaka

IS 4101 – Final Year Project in Informatioon Systems

Degree of Bachelor of Science Honours in
Information Systems

University of Colombo School of Computing
35, Reid Avenue, Colombo 07,
Sri Lanka
April 2024

Table of Contents

Contents

1 Introduction

Meetings are vital for any organization as they enable collaboration, decision-making, and the exchange of crucial information. However, to ensure their success, meetings must be carefully planned and organized. This involves addressing key questions: Do we truly need to hold a meeting? Who should be invited? And what is the best format for the meeting — online, onsite, or hybrid ?

The Changing Landscape of Meetings: Before the COVID-19 pandemic, discussions about meeting security and privacy were less prevalent, as most meetings were conducted onsite with the physical presence of attendees. The pandemic has significantly altered this landscape, expanding meeting modes to include online and hybrid formats, in addition to traditional onsite meetings. Since 2020, the usage of online meeting platforms has surged due to quarantine restrictions and the need for remote collaboration (Jo et al. 2021).

Security and Privacy Concerns: The shift towards online and hybrid meetings has brought security and privacy issues to the forefront. In the Information Technology sector, many participants possess a sound understanding of information security (Golkarnarenji and Ali 2012). However, even knowledgeable individuals can make errors, especially as the complexity of the scenarios increases (Culafi 2023). Human decision-making is often influenced by emotions and biases, which can lead to mistakes. This is equally applicable in the context of organizing meetings, where improper use of online platforms can result in financial, reputational,and losses of proprietary information, capital and corporate value.

Selecting the Right Participants: One of the most critical aspects of organizing a meeting is inviting the right participants. Although this may seem straightforward, it is often a rushed or overlooked step. The success and productivity of a meeting largely depend on having the appropriate individuals present, whether in person or virtually. Selecting the right attendees is crucial because their background and capabilities can influence the meeting's mode and effectiveness. Moreover, having the right participants is essential for maintaining the confidentiality of the information shared during the meeting. When only the necessary and relevant individuals are present, the risk of information leakage is minimized, and sensitive discussions can be conducted securely. Cognitive and organizational bias undermines good decision-making.

To ensure a successful and secure meeting, consider the following principles for selecting participants:

1. **Need**: Identify who is essential based on their relevance to the meeting's topic and their ability to contribute significantly to the discussions. These are the individuals whose presence is crucial for the meeting's success and whose involvement ensures that confidentiality is preserved.

2. **Want**: Differentiate between those whose presence is desired but not critical. While these individuals might add value, they are not essential unless they can provide meaningful contributions to the meeting's agenda and help maintain the meeting's confidentiality.

3. **Value**: Assess the potential value each attendee brings. The goal is to ensure

that all participants can contribute to achieving the desired outcomes, whether that involves making decisions, offering insights, or advancing solutions. Their involvement should also align with the need to safeguard the information discussed.

By carefully selecting participants based on need, want, and value, you align the attendees with the meeting's goals, ensuring that each meeting is productive and purposeful. Clear objectives will guide you in choosing the right people, leading to more effective and efficient meetings. Moreover, this thoughtful selection process enhances the confidentiality of the information shared, ensuring that sensitive topics remain secure and are only accessible to those who are truly relevant.

Accordingly, during our research project, we will explore whether it is possible to identify a relationship among security and privacy-related factors of a meeting including participants, capabilities of participants, documents, and data shared in the meeting and meeting mode. After identifying such a relationship, we expect to evaluate conformance of the relationship with real world scenarios accurately. Then future researchers will be able to use our findings with confidence, to proceed further in our research path associated with meeting security and privacy.

2 Background, theory, related work, research gap and statement of the problem

2.1 Background

Meetings are an integral part of organizational operations, serving as platforms for collaboration, decision-making, and the exchange of essential information. Traditionally, most meetings were conducted onsite, with participants physically present in a designated location. However, the COVID-19 pandemic has transformed the landscape of how meetings are held, leading to a significant rise in online and hybrid meeting formats. This shift has brought new challenges and considerations, particularly concerning the security and confidentiality of information shared during meetings.

Prior to the pandemic, meetings were mainly held in person, and security concerns were largely physical — ensuring that meeting rooms were secure and that unauthorized persons were not present. The rapid adoption of online meeting platforms since 2020 has necessitated a reevaluation of these security paradigms (Jo et al. 2021). The ”new normal” of remote work has highlighted the vulnerabilities inherent in digital communications, with security breaches and privacy issues becoming more frequent and complex (Bispham et al. 2021)(Ozer et al. 2024).

The increase in remote work and the reliance on online meeting platforms have led to a spike in reported security incidents (Jo et al. 2021)(Bispham et al. 2021). These platforms, while convenient, have been found to have various security flaws, ranging from phishing attacks to unauthorized access and data breaches (Ozer et al. 2024). Early in the pandemic, many popular meeting platforms faced inspection over their inadequate security measures, which were quickly exploited as their usage increased (Jennings 2021). Although improvements have been made, the challenge of securing online meetings remains prominent. However, irrespective of the meeting mode, any opportunities given to the wrong attendees for the meeting can give room for the insecurity of the meeting and the attack surface can be increased.

Research into the security issues associated with the ”Work From Home” culture has shown a marked increase in vulnerabilities, particularly in digital communication tools. Studies indicate that phishing and other cyberattacks have targeted the expanded digital workspace, exploiting both technological and human weaknesses (Salloum et al. 2021). Furthermore, while the security of online meetings has received significant attention, there is a noticeable lack of comprehensive strategies addressing the secure organization and execution of meetings based on the sensitivity of the information discussed and the selection of participants.

A critical aspect of meeting organization is the selection of participants. Ensuring that the right people are invited to a meeting is not only a matter of operational efficiency but also of maintaining the confidentiality and security of the information shared. Inappropriate or unnecessary attendees can increase the risk of information leakage and compromise the meeting's objectives. Therefore, a systematic approach to selecting participants, based on their relevance and the nature of the information being discussed, is essential for maintaining security (“How to Decide Who Should Attend Your Meeting?” 2024).

2.2 Theory

For now, based on our literature survey, we can suggest Meeting Science — the formal, systematic investigation into pre-meeting processes, during-meeting processes and post-meeting processes, in order to get optimum advantages of a meeting, and Media Naturalness Theory — the natural tendency of people to attend onsite meetings due to various needs like co-location of participants, observing participants' body language, observing their facial expressions etc. as the theories that would be useful for us, to identify the relationship among meeting factors (Karl, Peluchette, and Aghakhani 2021). These theories will be supportive frames of reference for our research, aiding in our understanding of meeting contexts. However, our research will not be directly grounded in the aforementioned theories.

2.3 Related work

Before 2020, researchers have tried to show how security violations and data breaches can occur considering general information security, but without especially focusing on online meetings. For example, research shows how violations can occur if a user uses a browser, instead of a meeting platform application, to attend an online meeting (Kumar et al. 2017). Regarding other features such as the usability and efficiency of online meeting platforms, there was almost no research published. In addition, researchers have not noticeably attempted to compare features of different meeting platforms before covid-19 pandemic.

After covid-19 pandemic, there is research carried out to evaluate the security and privacy of online meeting platforms (Hasan and Hasan 2021)(Isobe and Ito 2021). Especially, many research focused on the security and privacy of online meetings, though only a few selected examples are cited in our proposal document. Further studies have been carried out to compare the features of different meeting platforms as well (Arishina, Hu, and Hoppa 2022). In addition, there is research conducted to analyze the effectiveness of online meetings vs onsite meetings, based on the situation (Karl, Peluchette, and Aghakhani 2021).

Though these kinds of research have been conducted by researchers separately, with several distinct goals, it can be observed that there was no attempt to propose an acceptable scientific mechanism for reducing the overall risk surface associated with meetings, in aspects of security and privacy (Tondel and Cruzes 2022). In other words, still, research has not been conducted to observe the possibility of developing a proper methodology to support the decision-making process regarding the confidentiality of meetings. Therefore, the lack of research work in exploring behaviors of meeting factors associated with security and privacy leads to a research gap.

2.4 Research gap

After analyzing the literature, we have identified the lack of a reliable decision-making mechanism for arranging meetings with the appropriate participants in the right meeting mode as a significant issue. This makes room for sensitive information discussed in the meetings to be vulnerable to various data breaches. To address this massive issue, as the initiative research gap, it is a must to identify whether there is an evidently provable relationship among **meeting mode, participants and their capability levels, and information exchanged in meetings**. If a relationship can be identified among such factors, then it should be expressed in a formal manner, for evaluating its validity and accuracy.

So, we hope to address this initiative research gap within our research project, and to evaluate our findings at the end, to prove the acceptability of those findings.

2.5 Statement of the problem

The shift to online and hybrid meeting formats has raised significant concerns regarding security and privacy(Jo et al. 2021)(Bispham et al. 2021) of meetings. While traditional onsite meetings offered a controlled environment, the complexity of meeting requirements and human factors pose vulnerabilities, leading to potential financial and data losses. Additionally, the importance of selecting the right participants for meetings has been underscored, yet it often remains overlooked. Therefore, there is a critical need to investigate the relationship among security and privacy factors, including participant selection, their capabilities, information shared, and meeting modes, to develop evidence-based strategies for mitigating risks.

Accordingly, our concise problem statement is;

There is a need to investigate whether a demonstrable relationship exists among meeting modes, information exchanged during meetings, and participants and their capability levels.

3 Statement of the research question

3.1 Research question

- How to prove the hypothesis stating that meeting participant selection is primarily dominated by the documents presented and that the choice of meeting mode depends on the participants' capabilities and the information within those documents?

4 Project aims and objectives

4.1 Project aims

1. Assessing the validity of assumed hypothesis.
2. Based on validity, expressing a relationship among security and privacy-related meeting factors.
3. Measuring the conformance of the identified relationship with real world scenarios accurately.

4.2 Objectives

1. Conducting a thorough case study and a data analysis to assess the validity of hypothesis.
2. Deep investigation into data gathered, regarding meetings to identify a relationship
3. Proposing a reliable method to measure the conformance of the identified relationship with real world scenarios.

5 Planned research approach and evaluation plan

Research type: Inductive reasoning - Grounded theory research

Research strategy: Exploratory research

Assumption: As a pre-meeting requirement, we assume that documents containing the agenda, and information to be discussed in the meeting will be created with different access control levels.

Hypothesis: Meeting participant selection is primarily dominated by the documents presented, and the choice of meeting mode depends on the participants' capabilities and the information within those documents.

Since a relationship among security and privacy-related meeting factors has not been explored yet in research, our research is an exploratory research. In this, both quantitative and qualitative data will be analyzed by us.

5.1 Planned research approach

Research methodology: Convergent Parallel Mixed method research

1. Case study on meetings as background research
2. Data collection
3. Data interpretation

4. Investigation on relationships in interpreted data
5. Evaluation of the relationships for conformance with real world scenarios

5.2 Evaluation plan

The identified relationship among meeting documents, meeting mode, meeting participants and participants' capabilities will be evaluated by investigating the level upto which it conforms to the real world scenarios accurately.

6 Scope, delimitations and justifications

6.1 In scope

Impact of document characteristics: Analyzing how document type (agendas, reports, etc.), content (information complexity, collaboration needs), and accessibility (online/offline availability) influence meeting mode decisions (onsite vs. online).

Document security considerations: Exploring how document confidentiality and security concerns (e.g., sensitive information, leak prevention) affect the decision-making process for meeting format.

Participant selection based on document sensitivity: Analyzing how the confidentiality and security classification of documents (e.g., public, confidential, top secret) influence the selection of participants for meetings that will discuss them. This will explore how document sensitivity dictates who needs access to the information for the meeting to be productive. The way how capability level of the participant is incorporated into the participant selection process also will be analyzed by us.

Participant categorization for access control: Investigating how meeting participants are categorized based on factors like their roles (manager, team member), departments, and clearances (security levels). This categorization will determine what access permission levels (read-only, edit, etc.) they receive for the documents associated with the meeting.

6.2 Out of scope

Specific meeting platform features: We will focus on the meeting modes such as online, onsite and hybrid, but not on different online meeting platforms currently available.

Meeting decision-making process in detail: While the research will touch upon how confidential documents influence decisions related to meeting security and privacy, it will not dive deeply into the entire meeting decision-making process including many other factors such as cost-effectiveness, efficiency etc.

Implementation of a usable decision support system: The primary focus of this project is on the conceptual aspects of online meeting security, emphasizing a comprehensive understanding of the research gap, rather than diving into the technical implementation or the development of a specific usable product.

7 Research contribution to Information Systems and benefits to the society

7.1 Research contribution to Information Systems

This project addresses a common issue in the field of information systems: safe and effective meeting administration, particularly concerning the sharing of confidential information. We will conduct an in-depth study into how meetings are influenced by the capabilities and backgrounds of the participants which has not been done so far. Through this research, we aim to reduce the cognitive workload of meeting organizers in organizing meetings while ensuring privacy and confidentiality of shared information. This will help minimize manual errors that may occur during meeting arrangements.

The use of a rule-based approach for participant classification enhances the field by optimizing meeting lineups and ensuring the participation of the correct stakeholders. Together, this research opens up new perspectives for considering various aspects of meeting modes. Overall, this research aims to enhance the field by providing a strong foundation for handling and safeguarding sensitive data in meetings.

7.2 Significance of the project

This research project will be significant relative to other similar work referred to in the literature survey, because currently there is no research that has paid attention to check the possibility of implementing a standard mechanism to reduce the risk surface of meetings, by supporting the meeting organizing process concerning meeting modes, information exchanged in meetings, and participants and their capability levels. Based on our literature survey, all related work has focused on analyzing the security and privacy of existing online meeting platforms and manifesting the importance of selecting the correct meeting mode based on theories like Meeting Science and Media Naturalness theory (Karl, Peluchette, and Aghakhani 2021)(Hasan and Hasan 2021)(Isobe and Ito 2021). Our literature survey shows some research that has mentioned this gap, as future work (Tondel and Cruzes 2022).

Ultimately, the significance of this research project is that, this is the initiative step of paving the way to implement a reliable decision support methodology, for helping the meeting organizing process, in aspects of security and privacy.

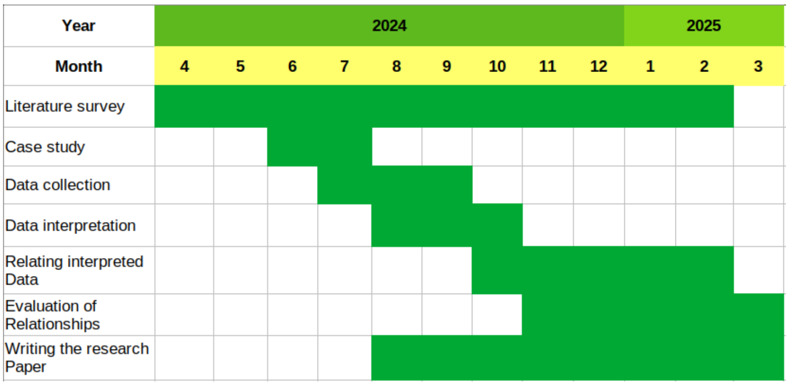
7.3 Benefits to the society

From the literature survey we conducted, it is found that none of the research has been conducted to implement a rule logic to enhance the security of meetings by assessing the risk factors based on the data circulated within the meeting. So this initiative has significant positive social effects. The research outcomes will aid the people in reducing the cognitive load while organizing meetings. Enhancing the safety and effectiveness of both virtual and hybrid meetings, the initiative contributes to the increasing popularity of remote work, which has turned into an essential component of modern professional life. This approach will also facilitate meeting organization for individuals with limited expertise in aiding to select the right meeting mode based on the participant's nature and sensitivity of information shared reducing the manual work. When cyber dangers are on the rise, enhanced meeting security helps preserve privacy and confidence in digital communications by protecting critical information. Effective participant classification maximizes time and resource utilization, which raises output and increases job satisfaction. Additionally, encouraging remote work via safe technologies lessens the need for travel, which lowers carbon footprints and promotes environmental sustainability. In the end, by encouraging safe, effective, and sustainable work habits, this research significantly benefits society on both a professional and personal level.

Furthermore, future enhancements could involve integrating the outcomes of this research into real-time meeting platforms, potentially increasing user trust in online meetings.

8 Project timeline and current progress

8.1 Project timeline



Year	2024									2025		
Month	4	5	6	7	8	9	10	11	12	1	2	3
Literature survey	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	
Case study			🟩	🟩								
Data collection				🟩	🟩	🟩						
Data interpretation					🟩	🟩	🟩					
Relating interpreted Data							🟩	🟩	🟩	🟩	🟩	
Evaluation of Relationships								🟩	🟩	🟩	🟩	🟩
Writing the research Paper					🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩

Figure 1: Planned project timeline

8.2 Current progress

Currently literature survey and case study are going on, in parallel.

List of References

References

Arishina, Y., Hu, Y.F., and Hoppa, M.A. (2022). “A Study of Video ConferencingSoftware Risks and Mitigation Strategies”. In: *Journal of The Colloquium for Information Systems Security Education* 09, pp. 1–10. DOI: `https://doi.org/10.53735/cisse.v9i1.134`. URL: `https://cisse.info/journal/index.php/cisse/article/view/134/134`.

Bispham, M.K., Creese, S., Dutton, W.H., Esteve-Gonzalez, P., and Goldsmith, M. (2021). “Cybersecurity in Working from Home: An Exploratory Study”. In: *SSRN Electronic Journal* January 2021, pp. 1–43. DOI: `https://doi.org/10.2139/ssrn.3897380`. URL: `https://www.researchgate.net/publication/353661008_Cybersecurity_in_Working_from_Home_An_Exploratory_Study`.

Culafi, A. (2023). “Microsoft AI researchers mistakenly expose 38 TB of data”. In: *TechTarget*. URL: `https://www.techtarget.com/searchsecurity/news/366552399/Microsoft-AI-researchers-mistakenly-expose-38-TB-of-data`.

Golkarnarenji, G. and Ali, U. (2012). “Unified Communications Security : A study of IT personnel awareness on video conferencing security recommendations”. In: *Department of Computer science, Electrical and Space Engineering, Lulea University of Technology*, pp. 1–114. URL: `https://www.academia.edu/3056220/Unified_Communications_Security_A_study_of_IT_personnel_awareness_on_video_conferencing_security_recommendations`.

Hasan, R. and Hasan, R. (2021). “Towards a Threat Model and Security Analysis of Video Conferencing Systems”. In: *IEEE Consumer Communications Networking Conference (CCNC)* 01, pp. 1–4. DOI: `https://doi.org/10.1109/CCNC49032.2021.9369505`. URL: `https://www.researchgate.net/publication/349994212_Towards_a_Threat_Model_and_Security_Analysis_of_Video_Conferencing_Systems`.

“How to Decide Who Should Attend Your Meeting?” (2024). In: *Condeco*. URL: `https://www.cnbc.com/2021/08/01/zoom-reaches-85-million-settlement-over-user-privacy-and-hacker-zoombombing.html`.

Isobe, T. and Ito, R. (2021). “Security Analysis of End-to-End Encryption for Zoom Meetings”. In: *IEEE Access* 09, pp. 90677–90689. DOI: `https://doi.org/10.1109/ACCESS.2021.3091722`. URL: `https://ieeexplore.ieee.org/document/9462825?denied=`.

Jennings, R. (2021). “Zoom fails grow: 530,000 passwords leaked, details for sale by hacker”. In: *TechBeacon*. URL: `https://techbeacon.com/security/zoom-fails-grow-530000-passwords-leaked-details-sale-hacker`.

Jo, J., Chae, Y., Jang, H., and Kong, J. (2021). “Federated-Access Management System and Videoconferencing Applications: Results from a Pilot Service during COVID-19 Pandemic”. In: *Multidisciplinary Digital Publishing Institute (MDPI)* Electronics 2021,10, 2239, pp. 1–19. DOI: `https://doi.org/10.3390/electronics10182239`. URL: `https://www.researchgate.net/publication/354545424_Federated-Access_Management_System_and_Videoconferencing_Applications_Results_from_a_Pilot_Service_during_COVID-19_Pandemic`.

Karl, K.A., Peluchette, J.V., and Aghakhani, N. (2021). “Virtual Work Meetings During the COVID-19 Pandemic: The Good, Bad, and Ugly”. In: *Sage* 53(3), pp. 343–365.

DOI: https://doi.org/10.1177/10464964211015286. URL: https://journals.sagepub.com/doi/full/10.1177/10464964211015286.

Kumar, S., Mahajan, R., Kumar, N., and Khatri, S.K. (2017). "A study on web application security and detecting security vulnerabilities". In: *IEEE* 09, pp. 451–455. DOI: https://doi.org/10.1109/ICRITO.2017.8342469. URL: https://ieeexplore.ieee.org/document/8342469.

Ozer, M., Kose, Y., Kucukkaya, G., and Varlioglu, E.R. (2024). "The Shifting Landscape of Cybersecurity: The Impact of Remote Work and COVID-19 on Data Breach Trends". In: *IEEE Computer Science and Computer Engineering (CSCE)*. URL: https://arxiv.org/html/2402.06650v2.

Salloum, S., Gaber, T., Vadera, S., and Shaalan, K. (2021). "Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey". In: *Procedia Computer Science* 189, pp. 19–28. DOI: https://doi.org/10.1016/j.procs.2021.05.077. URL: https://www.sciencedirect.com/science/article/pii/S1877050921011741.

Tondel, I.A. and Cruzes, D.S. (2022). "Continuous software security through security prioritisation meetings". In: *Elsevier* 194, pp. 1–25. DOI: https://doi.org/10.1016/j.jss.2022.111477. URL: https://www.sciencedirect.com/science/article/pii/S0164121222001625.