

Anonymity Enhancing Technologies (AETs) in GDSS Supported Meetings

Amer Al shishany, Jackson Adams
Essex Business School
University of Essex
Wivenhoe Park, Colchester, CO4 3SQ, U.K
[asalsha, khala}@essex.ac.uk](mailto:asalsha,khala}@essex.ac.uk)



ABSTRACT: *Using the anonymity feature of GDSS (Group Decision Support Systems) meeting application as a backbone, this paper is aimed to find out whether enhancing technical anonymity in the GDSS supported meetings will increase participants' confidence in the software's confidentiality, causing more productive discussions. Some Anonymity Enhancing Technologies (AETs) are discussed, and their impact on ensuring anonymity is investigated. Semi-structured interviews were conducted with experienced facilitators, technical support individuals and users of GDSS meeting software, from real business environmental settings. The 'FacilitatePro' and 'MeetingSphere' meeting applications were investigated for the research. The paper illustrates some results, and proposes future research related to AETs in GDSS supported meetings.*

Keywords: Anonymity Enhancing Technologies (AETs), Anonymity, Group Decision Support Systems, Strategic Component of the SIDE Theory

Received: 8 November 2012, Revised 14 December 2012, Accepted 20 December 2012

© 2013 DLINE. All rights reserved

1. Introduction

The GDSS is a complex technology that provides number of features for enhancing communication among meeting members, such as anonymous idea listing, voting techniques and comments recording [5], which helps to structure meetings in brainstorming and voting sessions [4]. One of the critical features the Decision Support Systems provide is anonymity, which allows participants to exchange generated ideas anonymously (5, 24, 18), freeing members of the group from the influences of other high ranked or powerful individuals [34, 22] and evaluating members' contributions and ideas based on the idea's value, not on the author's status [13].

Group Support Systems is divided into four configurations: Same Time / Same Place; Same Time / Different Place; Different Time / Same Place; and Different Time / Different Place [15, 19]. This paper is limited to investigate meetings conducted in the 'Same Time / Same Place' configuration, which is considered to be an important type of meeting due to its role in establishing social relations, team milestones and dealing with major changes in decision making tasks [4].

In this type of GDSS supported meetings group members gather around a discussion conference table, each group member has his own computer terminal linked to other terminals by a computer network. The meeting is guided by a facilitator; who holds the duties of running the session, categorizing and prioritizing the questions and the suggested solutions by the meeting members. Participants' comments, contributions and other meeting procedures appear, anonymously, on each

members screen and/or on a shared large display screen fitted at the front of the participants [15].

2. Motivation for The Research

Anonymity in GDSS organizes meetings and provides the users with the possibility to remain unidentifiable [3]. Unfortunately, sometimes, users of such systems do not accept these technologies' constraints, instead, they try to attribute comments to their authors [12], modify, adapt or exploit the available technology to suit their own needs and achieve their own goals [4] 'working-around' the system [14].

Even though, the GDSS application organizes how users and groups communicate, some users of these systems remain suspicious of the security and the secrecy levels that these applications maintain. This situation may negatively impact the willingness of participants to freely contribute to the discussions and dissent other group members or express their ideas without fear [22], consequently, reducing the effectiveness of the GDSS system [8]. It is vital to understand how these technologies establish anonymity, and how GDSS meeting participants utilize anonymity strategically [9] to resist and dissent powerful members [23].

3. Theoretical Framework: The Strategic Component of The SIDE Theory

Arguably, the Social Identity model of Deindividuation Effects (SIDE) theory is the most current and influential theory in terms of anonymity and group members interpersonal interaction [3]; it tries to provide an explanation for the impacts of anonymity and identifiability on group behavior in CMC (Computer Mediated Communication) environment [22]. To explain how anonymity impacts CMC the SIDE theory encompasses two aspects: Cognitive and Strategic [3].

The Cognitive aspect of the SIDE theory focuses on how group and individual behavior within a group is mediated by anonymity, and focuses, as well, on individual identifications strength within the group [16, 22, 3]. While the strategic aspect of the theory explores how members of groups intent to strategically exploit and use the anonymity feature of a computerized meeting application, [30, 3].

The strategic component of the SIDE theory has received scant scholarly attention, and needs further investigation [3, 22]. It argues that, when individuals perceive how anonymity within computer mediated communication impacts interpersonal communication, they start to exploit and utilize anonymity, strategically, using different strategies, to achieve their own objectives and needs [23, 30, 3]. For example, groups with low power status may utilize this feature for resisting the powerful majority, in this way group members are able to utilize anonymity to express their ideas and point of views, which could be contradictory to the ideas of other powerful group members. The strategic component of this theory, also proposes that, anonymity in communication via computers supports and fosters resistance [22].

4. Anonymity in GDSS Meetings: Technical Anonymity

Anonymity has been categorized under two broad categories: Technical and Social anonymity [12]. The social category refers to the participant's self-perception as unidentifiable or anonymous in a social context to himself and to others; due to lack of cues that may attribute participants' identity. The technical category refers to the removal of participants' names or any related identification information that may uncover the author's identity in an electronic material exchange [3]. [8] referred to this technical anonymity as 'Procedural Anonymity' which deals with the technical aspect of ensuring the anonymity of communication among participants using special network protocols to hide the source's identity.

However, users of the GDSS meeting applications realize and fear that anything they may say within these meetings could be archived, tracked and linked to them. Therefore, so called Privacy-Enhancing Technologies were developed [9]; in attempt to eliminate those fears and to provide some kind of protection for both the participants' identities and the data being transferred over the network.

5. Anonymity Enhancing Technologies (AETS) in GDSS Meetings

Anonymity has been defined as "the state where a user is not identifiable when using a resource or service" [25] and as "the degree to which a communicator perceives the message source as unknown and unspecified" [2]. In anonymous

communication, also known as unlinkable anonymity, the communicating parties are unknown, unidentifiable and can't be remembered [1].

The amount of research dealing with technologies and mechanisms to enhance anonymous online communication interactions is quite large. This section will be discussing only some of these technologies which companies providing GDSS meeting applications promote as being the most highly secured and sophisticated applications. These Anonymity Enhancing Technologies (AETs) foster the anonymous interaction across the network system and aim at masking users' identities and their comments or contributions during and after the meetings. Data Encryption and Data Transfer Protocol techniques being the two primary mechanisms used by the GDSS software providers are discussed. The iPad devices as a new emerging technology in the GDSS meeting environment and their impact on enhancing anonymity, is discussed, as well.

5.1 Data Encryption

The first class of AETs, used by the GDSS meeting applications is the 'Data Encryption' technique. Data Encryption is the primary mechanism used to maintain secrecy and confidentiality [8] over the GDSS supported meeting application. The data encryption technique helps to protect both users' identities, and the data being transferred through the network from being tracked, hacked or disrupted. All transmissions over the network consists of three components; a header revealing the source or the sender's address, the next destination or receiver's address and the encrypted message itself, which can be read, by the next recipient, only. Therefore all messages being transmitted over the network must be encrypted; ensuring end to end privacy, which allows only the intended recipient to be able to read the content of the message. However, this technique does not guarantee full anonymous communication [8].

5.2 Data Transfer Protocol – SSL (Secure Socket Layer)

The second class of AETs is the Data Transfer Protocol, which the GDSS system uses to protect the data being transmitted over the computer network. As the internet network being used by the GDSS meeting applications to transfer data through its network clients and server, it becomes important that the contents of these transactions will be protected through the net. Though without problems, SSL (Secure Sockets Layer) is one of the most widely used privacy enhancing technologies on the internet, and originally used for secure interactions over the public internet network, but afterwards has been applied to file transfer, telnet and news services [27]. One of the reasons for SSL technology success stems from its compatibility with the major web browsers [10].

These GDSS meeting applications seek both data anonymity and connection anonymity. Data anonymity is "*filtering any identification information out of the data that is exchanged in a particular application*", and connection anonymity is "*hiding the identities of source and destination during the actual data transfer*" [6]. To achieve this objective the 'FacilitatePro' and the 'MeetingSphere' applications use the SSL technology, to protect, both, the identities of the user and the data being transmitted over the system's network. SSL protocol, authenticates, creates an encrypted communication channels and enables servers and clients to encrypt data being transmitted between an individual client and a server.

In sum, SSL is the encryption mechanism that protects on line transactions [11] allowing the encrypted data to travel over the network securely [29], without being worried that this data is being transmitted in plain text (Spitalnick, 2009). Even though, achieving relative anonymity is possible, yet, remaining truly anonymous, on line, has been unsolved problem [26].

5.3 IPAD Devices in I-labs

The iLab is Innovation Laboratory – "*an inspirational innovative facility designed to transport users from their everyday environment into an extraordinary space encouraging creative thinking and problem solving*", including anonymous brainstorming software and the use of a variety of facilitation techniques to stimulate and capture this participants discussion and idea generation process (<https://ilabnet.essex.ac.uk/mod/glossary/view.php?id=18>).

One of the problems associated with the physical proximity of participants within the iLab sessions is the ability of participants to see and hear each other when typing their comments, by observing and hearing the keyboard strokes, especially when there is only one person typing alone, and eventually participants are able to attribute comments that have just displayed on the shared screen with the authors. Enhancing the iLab sessions' anonymity by installing iPad devices to the sessions, to take over the laptops place, may be considered one of the effective solutions for the keyboard strokes sound problem, because the iPad has enabled touch screen keyboard.

Installing iPads to the iLab environment was an idea generated by the iLab facilitator at the Southend campus of the

University of Essex in UK. The reason for purchasing and implementing the iPads was not for anonymity enhancement purposes, but, rather to keep the iLab updated in terms of the technological devices used within the iLab, and to give participants more physical space to move and sit wherever is convenient for them; because the iPads are Wi-Fi connected to the system.

6. Research Method

Semi-structured interviews, as the most commonly used kind of interviews in small scale social research [32] and as one of the best data collecting tools used in Information Systems (IS) research [20], have been conducted with three categories: Software Users, Facilitators of iLabs and Technical Support experts. The '*FacilitatePro*' provided by the (Facillitate.com) and the '*MeetingSphere*' provided by the (MeetingSphere.com) applications were used for this research.

Software users category were individuals from both genders and have used the GDSS meeting software more than once; their occupations ranged from normal staff users to head of department. The facilitators were experienced iLab facilitators whom have more than three years of experience in maintaining and facilitating sessions within the iLabs and whom have been, previously, normal users of the software within their meetings. The last group was highly qualified technical support individuals who have the responsibilities of running the software technically within the iLabs and coordinating with the companies providing the software.

A number of 13 subjects were interviewed and each interview lasted for, approximately, one hour. Three categories of questions were formulated; each category covered issues related to the specific position of the subject as being a user, a facilitator or technical support. The users' interviews covered issues related to the usage of the software and participants' interactions with the anonymity feature of the software. While the facilitators' questions investigated issues relevant to the experience from facilitating sessions and observing participants behavior during the sessions within the meeting room with the software or other meeting facilities within the iLab. The technical support interviews were more related to the technical issues of the software itself, such as, the Data Encryption and Data Transfer Protocols. A comprehensive deep image was constructed from interviewing those three groups of users for the GDSS meeting application.

7. Findings and Suggestions for Future Research

Understanding how anonymity is perceived by meeting participants, and how they interact with it is a vital issue towards improving the outcomes of GDSS meetings. All this research subjects; users of the software, facilitators of the iLabs and even technical support experts were found unaware of the '*Data Encryption*' level or the '*Data Transfer Protocols*' used within these systems. Therefore, promoting and enhancing these ATEs, within (Same Place / Same Time) GDSS meetings configuration, is not of a significant impact in fostering participants' willingness to dissent others or to increase participants' confidence in the anonymity of the iLab environment.

Another finding for this research is that installing iPad devices may enhance the physical anonymity in the iLab environment and could be useful to overcome the issue of some participants being able to attribute comments, caused by the physical proximity in the GDSS meetings. However, usually participants were found to be task focused and not so keen to attribute comments. The issue of attributing comments was not of a major concern neither for the users nor for the facilitators.

Overall, for the purpose of future research, this study encourages other researchers to investigate one of the GDSS meeting applications' feature, which provides the ability to conduct a meeting with participants from different locations at the same time (Same Time / Different Places), without the need for participants to physically move to one specific meeting room. This feature was found not used yet by the iLab service providers because of the lack of demand by clients on such service. Investigating this (same time / different places) configuration is a good challenge, and could yield some new findings in terms of using previously mentioned AETs in this kind of GDSS supported meetings.

References

[1] Alam^ˆaki, T., orksten, M. Bj^ˆ, Dornbach, P., Gripenberg, C., Gyoerbio, N., Marton, G., Nemeth, Z., Skyttae, T. (2003). Privacy Enhancing Service Architectures, p. 99-109. *In*: Second International Workshop, PET, San Francisco, CA, USA, Roger Dingledine and Paul Syverson (Eds.) Revised Papers, Springer.

- [2] Anonymous. (1998). To Reveal or Not to Reveal: A Theoretical Model of Anonymous Communication, *Communication Theory*, 8 (4) 381-407.
- [3] Christopherson M. Kimberly. (2007). The positive and negative implications of anonymity in Internet social interactions: On the Internet, Nobody Knows You're a Dog, *Computers in Human Behavior*, 23, 3038-3056.
- [4] Daniel, Levi. (2007). *Group Dynamics for Teams*, 2nd Ed, Sage Publications, Inc.
- [5] DeSanctis, Gerardine, Poole, Marshall Scott, Zigurs, Ilze, DeSharnais, George, D'Onofrio, Marianne, Gallupe, Brent, Holmes, Michael, Jackson, Brad, Jackson, Michele, Lewis, Howard, imayem, Moez, Lee- Partridge, JooEng, Niederman, Fred, Sambamurthy, V., Vician, Chelley, Watson, Richard, Billingsley, Julie, Kirsch, Laurie, Lind, Rebecca, Shannon, Dale. (2008). The Minnesota GDSS Research Project: Group Support Systems, Group Processes and Outcomes, *Journal of the Association for Information Systems*, 9 (10) 551-608.
- [6] Diaz, C., Seys, S., Claessens, J., Preneel, B. (2002). Towards measuring anonymity. In: Second International Workshop, PET, San Francisco, CA, USA, Roger Dingledine and Paul Syverson (Eds.) Revised Papers, Springer.
- [7] Flanagan J. Andrew, Tiyaamornwong Vanessa, O'Connor Joan, Seibold R. David. (2002). Computer-Mediated Group Work: The Interaction of Sex and Anonymity, *Communication Research*, 29 (66).
- [8] Gavish, B. A., Gerdes J. H. Jr. (1998). Anonymous mechanisms in group decision support systems communication, *Decision Support Systems*, 23, 297-328.
- [9] Goldberg Ian. (2002). Privacy-enhancing Technologies for the Internet, II: Five Years Later, In Workshop on Privacy Enhancing Technologies, Lecture Notes in Computer Science 2482, p.1-12. Springer-Verlag.
- [10] Goldberg Ian. (2007). Privacy-Enhancing Technologies for the Internet III: Ten Years Later, chapter 1 of Digital Privacy: Theory, *Technologies and Practices*, p. 3-18. Auerbach, December.
- [11] Greene, Tim. (2011). With SSL, who can you really trust?, *Network World*, 28 (15).
- [12] Hayne C. Stephen, Pollard E. Carol, Rice E. Ronald. (2003). Identification of Comment Authorship in Anonymous Group Support Systems, *Journal of Management Information Systems / Summer*, 20 (1) 301-329.
- [13] Jessup, Leonard M., Connolly, Terry, Galegher, Jolene. (1990). The Effects of Anonymity on GDSS Group Process With an Idea-Generating Task, *MIS Quarterly*, 14 (3) 313-321.
- [14] Johnson, G. Deborah, Wetmore M. Jameson. (2009). *Technology and Society: Building Our Sociotechnical Future*, Massachusetts Institute Technology.
- [15] Klein E. Esther, Tellefsen Thomas, Herskovitz J. Paul (2007). The use of group support systems in focus groups: Information technology meets qualitative research, *Computers in Human Behavior*, 23, 2113-2132.
- [16] Lea Martin, Spears Russell, Groot de Daphne. (2001). Knowing Me, Knowing You: Anonymity Effects on Social Identity Processes within Groups, *Pers Soc Psychol Bull*, 27, 526.
- [17] Lee Eun-Ju. (2005). Effects of the Influence Agent's Sex and Self-Confidence on Informational Social Influence in Computer-Mediated Communication: Quantitative Versus Verbal Presentation, *Communication Research*, 32: 29.
- [18] Miranda M. Shila. (1994). Avoidance of Groupthink : Meeting Management Using Group Support Systems, *Small Group Research* February, 25 (1) 105-136.
- [19] Mittleman, D., Briggs, R. (1999). Communication technologies for traditional and virtual teams. In E. Sundstrom (ED), Supporting work team effectiveness, p.246-270.
- [20] Myers, Michael, D., Newman, Michael. (2007). The qualitative interview in IS research: Examining the craft, *Information & Organization*, 17 (1) 2-26.
- [21] Nunamaker, J. F., Jr., Briggs, R., Mittleman, D., Vogel, D., Balthazard, P. (1997). Lessons from a dozen years of group support systems research: A discussion of lab and field findings, *Journal of Management Information Systems*, 13 (3) 163-207.
- [22] Postmes, T., Spears, R. (2002) Behavior online: does anonymous computer communication reduce gender inequality?, *Personality and Social Psychology Bulletin*, 28 (8) 1073-1083.

- [23] Reicher, S. D., Spears, R., Postmes, T. (1995) A social identity model of deindividuation phenomena. In W. Stroebe & M. Hewstone (Eds.), *European review of social psychology*, 6, p. 161-198, Chichester, UK: Wiley.
- [24] Reinig A. Bruce, Mejias J. Roberto. (2004). The Effect of National Culture and Anonymity on Flaming and Criticalness in GSS-supported Discussion, *Small Group Research*, 35, 698.
- [25] Dritsas A. Stelios, Gritzalis A. Dimitris, Lambrinouidakis Costas. (2006). Protecting privacy and anonymity in pervasive computing: trends and perspectives, *Telematics and Informatics*, 23, 196–210.
- [26] Serjantov Andrei, Danezis George. (2003). Towards an Information Theoretic Metric for Anonymity, DR. Dingleline and P Syverson (Eds.), *Privacy Enhancing Technologies, Second International Workshop, CA, USA, April 14-15, 2002 Revised Papers*, Incs, p. 41-53, 2003, Springer-verlag Berlin.
- [27] Sidnie Feit. (1999). *TCP/IP: architecture, protocols, and implementation with IPv6 and IP security*, New York : McGraw-Hill, Signature ed., Rev. & expanded.
- [28] Spindler Torsten a, Wartmann Christoph a, Hovestadt Ludger a, Roth Daniel b, Gool Van Luc b and Steffen Andreas (2008) Privacy in video surveilled spaces, *Journal of Computer Security*, 16, 199–222, 199.
- [29] Spitalnick, Aaron (2009) Understanding Encryption and Its Role in Security, *CPA Practice Management Forum*, 5 (7) 5-10.
- [30] Spears Russell, Postmes Tom, Lea Martin, Wolbert Anka. (2002a). When Are Net Effects Gross Products? The Power of Influence and the Influence of Power in Computer - Mediated Communication, *Journal of Social Issues*, 58 (1) 91-107.
- [31] Spears Russell, Lea Martin, Corneliussen Arne Rolf, Postmes Tom, Haar Ter Wouter. (2002b). Computer-Mediated Communication as a Channel for Social Resistance: The Strategic Side of SIDE, *Small Group Research*, 33: 555.
- [32] Thomas Gray. (2011). *How to do Your Case Study, A Guide for Students & Researchers*, Thousand Oaks, CA: Sage Publications.
- [33] Valacich J. S., Jessup L. M., Dennis A. R., Nunamaker J. F. Jr. (1992). A conceptual framework of anonymity in group support systems, *Group Decision and Negotiation*, 1 _3, 219–241.
- [34] Wilson L. John, Griffin E. Thomas, Jessup M. Leonard. (2010). GSS Anonymity Effects on Small Group Behavior, *Academy of Information and Management Sciences Journal*, 13 (2).