國立雲林科技大學
99學年度博士班招生考試試題

系所別：資訊管理系
科　目：資訊管理文獻

Questions: **題目共有9題，作答時，請注意各題之比例配分並標示題號**

1. Please give the abstract, within 150 words in English, of this paper? (10%)

2. Based on the hypotheses (H1a-b to H3 a-b), please draw the research model, Figure 1, of this paper? (5%)

3. Given the structural equation modeling analysis, please draw the SEM results, Figure 2, of this paper? (10%)

4. Please indicate why author(s) included both the lurkers and the posters population in this study? (10%)

5. Please briefly describe the Self-Determination Theory (SDT) mentioned in this study (5%)

6. Restricted data collection from the subject, please criticize the way author(s) conducted this study. (10%)

7. Please write down where is the paper makes a new and significant contribution? (15%)

8. Could the paper benefit from expansion to help your future works? (Please write in details) (15%)

9. Please point out what does the paper provide evidence of real or potential application for information system practice? (20%)

Communications of the Association for Information Systems

The Decision to Share Information and Rumors: Examining the Role of Motivation in an Online Discussion Forum

I. INTRODUCTION

The Internet has emerged as an increasingly popular resource for information seekers and providers. Among the popular online stops for Internet users are online communities, which serve as communication portals that use the ubiquitous reach of the World Wide Web to connect people interested in a similar topic [Hagel and Armstrong 1997]. The background of these communities range from groups devoted to specific professional topics to groups centered on entertainment and pop culture. Certainly, content that is posted to online communities is not all equally credible. As anyone who has been granted writing privileges to the community forum can publish information, content can range from being widely acceptable and verifiable to being highly dubious at first glance. Despite the immediate lack of validity of unsubstantiated information, such as rumors, in certain communities, rumors are not only acceptable but also desirable. This study explores the drivers that influence a member's decision to share substantiated and unsubstantiated content with other online members.

The paper is organized as follows. First, the background for this research which positions this study is discussed. Next, a theoretical model for this study is posited, and the primary hypotheses of the study are presented. This is followed by a discussion of our research methodology, data collection procedures, instrument validation, analysis techniques, and the results. Finally, we conclude with the study's findings, its implications for research and practice, its limitations, and future research directions.

II. BACKGROUND

Although several classification schemas for categorizing online communities have been posited, most studies that have examined information/knowledge-sharing within online communities either treat them as a monolithic entity [e.g., Ridings et al. 2002] or have predominantly focused on one type of online communities, i.e., communities of practice [e.g., Ardichvili et al. 2003; Wasko and Faraj 2000; Wasko and Faraj 2005]. Recent studies on online communities have recognized the limitations of analyzing multiple online communities collectively as a monolithic entity. The premise of this study is that online communities are not monolithic entities with congruent goals. Much as IS researchers have classified decision support systems by contexts within which a system is applied and any decisional guidance is applicable [Holsapple and Whinston 1996], online communities differ by the contexts in which the sharing occurs. It is conceivable that due to goal incongruity, sharing behaviors observed in one type of an e-community (such as a community of practice) are not extendable or applicable to other types of e-communities (such as recreational communities or communities of interest [Rothaermel and Sugiyama, 2001]). For instance, sharing by individuals in professional communities may be encouraged by organizational norms and procedures [Constant et al. 1994], the sharing conducted in communities of interest may well be driven by other motivations. Therefore, in order to extend our understanding of sharing behaviors within the context of online communities it is crucial to examine this behavior in diverse settings with various objectives. To this end, this study extends the current understanding about the sharing behaviors of online members by examining this behavior in a topic-oriented online community, with a recreational goal, instead of a community of practice, with a learning goal, which primarily exchanges know-how or best practices.

Online Community Member Types: Two types of online community members are the subject of this research: the poster and the lurker. Schlosser [2005] differentiated between the two types of members by defining posters as those who post their experiences on the Internet and lurkers as those who read those postings without any expected contribution of their own. Although there is a natural similarity between lurkers and the notions of "free riders" and "social loafing" found in small group research [Wagner 1995], lurkers are not necessarily a drain on the community. All posters were part of the lurker subset at one point, and surveys indicate that many posters remained in the lurking shadows until they became more comfortable with the community [Preece et al. 2004]. But because posters are active contributors, at some point in the past they became sufficiently motivated to voluntarily make public his or her opinions, questions, and statements to the rest of the online community.

There are several important reasons to include both the lurkers and the posters population in this study. First, in order to have a complete understanding of the online communities, it is essential to examine all the members within the population. Lurkers are reported to be the majority members in an online community. The percentage of lurkers within an online community is estimated to range from 50 to 90 percent of the total membership [Katz 2003; Mason 1999; Soroka et al. 2003]. Although, prior studies have stated that the omission of "individuals who read but do not post" as a limitation to the study of active participants because a significant portion of an online population that has

an equal opportunity to post/share is omitted [Wasko and Faraj 2005, p.52], most of the scholarly work on online communities has predominantly focused on the active participants. Moreover, among the few IS studies which have included lurkers [Rafaeli et al. 2004; Ridings et al. 2006], only a few of them have directly compared lurkers and posters. Second, the posters contribute to a community's resource base by posting content, whereas the lurkers benefit by viewing the content contributed by others. Although both the posters and the lurkers create site traffic, these communities are developed and sustained primarily through the content produced by the posters. Therefore, the community administrators are constantly trying to attract "potential" posters who would actively participate in the community by sharing content which is of interest to other members. While the lurkers are in the background of the community, they still represent a sizable portion of the community and could serve as a recruitment pool from which "new" posters who can instill "new blood" into the community can be recruited. Therefore, one of the practical purposes of our research is to seek a better understanding of factors that might motivate people to share information in online communities. Finally, in order to understand the motivational drivers that could potentially encourage lurkers to share content, we first have to isolate the motivational differences between the posters and the lurkers which are contributing to their contrasting sharing behaviors (posting versus not posting). The literature posits various reasons for the difference in behavior, such as a distrust in the abilities of community members, less obligation toward social exchange [Preece et al. 2004; Ridings et al. 2006]. However, we premise that something motivationally must overcome those reasons for lurkers who eventually become posters, so we attempted to ascertain the perceptions of motivational influences for both parties. Ridings et al. [2006], one of the few studies to examine poster and lurkers, conducted a descriptive analysis to compare the lurkers' and posters' trust levels, need for social support, and need for exchanging information with an attempt to uncover why lurkers and posters use virtual communities. Unlike Ridings et al.'s study, this study attempts to uncover the nature and magnitude of association between the sharing behaviors and its key antecedents. More specifically, this study examines the impact of motivational and social influences on both the poster's and lurker's sharing behaviors which we believe is a contribution to the literature on online community sharing.

Sharing Content: Another unique aspect of this research is its focus on two types of content which separates this study from other literature on online sharing behaviors. This work differentiates between content by how freely available and verifiable it is. Content that is posted to a community forum but can be readily found at and verified by other sources is referred to as *information*. By contrast, content that is currently unsubstantiated but largely relevant to the community is referred to as *rumor*. Both information and rumors are commonly posted to online community forums, along with other posts containing opinion, speculation, requests for information, and a multitude of various mixtures of all the above. Although, information sharing within the online communities is well explored, the notion of rumor as a valuable online community resource is relatively novel. Therefore, what is still unexplored is what drives people to share unsubstantiated content, such as rumors, with other online community members.

A rumor, characterized as a proposition for belief of topical interest disseminated without official verification [Knapp 1944], is mostly viewed as scandalous, damaging, harmful, and malicious. Therefore, rumor literature, although very limited in scope, has often focused on "controlling" the damage caused by rumor mongering (e.g., [DiFonzo et al. 1994; Knapp 1944; Rosnow 1988]). In this study, we adopt a resource based perspective with regard to rumors and that, depending on the community, rumors can be an entertainment resource critical to the development and sustenance of an online community. Adopting this perspective does not imply that we are marginalizing the dark side of rumor mongering, but in an online community such as the one examined in this study, a community devoted to a university's intercollegiate athletic program, rumors serve very unique purposes.

Sports generally provide a fertile breeding ground for rumors which passionate sports fans are eager to share and consume. The trading deadlines, drafts, injuries to top players, firing of coaches, conflicts among team players are frequent occurrences within the sport industry. These events provide an environment which is conducive for rumor generation and transmission. Currently, the market for sports related rumors is predominantly fulfilled by the sports discussion boards where fans gather to share and consume rumors about their teams. For instance, a sports-based online community associated with one university generated 10,000 message postings a day during the unfolding of the scandal which involved their newly hired coach. One university with a prominent sports program has at least three unofficial Web sites which "offer the same type of material that is available on an athletic department site, but their nerve center is the message board," where fans can anonymously share information and rumors [Layden 2003]. The majority of these Web sites are developed around a business model supported by online advertisements accompanying the discussion forum, the goal of which is for visitors to view or click on the sponsored advertisements. The popularity of a certain Web site, and by association, the fee to advertise on the Web site, is at least partially dependent on the contributions of its community members which attract visitors to the site. Several popular sports Web sites (such as ESPN and Yahoo) have recently entered this market by creating rumor links on their official Web sites.

Rumor mongering on a sports message board satisfies the emotional, cognitive, and problem-solving needs of an ardent sports fan.

Emotional Needs: Rumors about a sport team provide fans a space between possibility and reality which temporally is very exhilarating and entertaining. It also provides fans with an outlet to share a rumor that they feel is comforting or exhilarating, this could be an attempt to validate their positive fantasizing or wishful thinking in order to savor the anticipation of a satisfying event" [Rosnow 1988, pg. 20]. Moreover, sharing rumors on a community message board can help mitigate the fans' anxieties related to the unfavorable rumors and provide enjoyment by sharing the favorable rumors.

Problem Solving Needs: The community message board is also used by fans as a platform for verifying the credulity of the rumors surrounding their sports team. The rumor literature has often positioned the rumor mongering process as a collective problem-solving transaction [Bordia and Rosnow 1998; Rosnow 1988]. Community members post rumors on the message board in anticipation of confirming the credulity of the rumor when it is collectively evaluated by the skeptical and/or more informed members of the community.

Cognitive Needs: Rumors on the message board quench the ardent fans' insatiable curiosity to know everything about their team even before it is covered by the mainstream media. The sports discussion boards are often breaking rumors days and months before a story is broadcasted in the news media [Layden 2003]. Moreover, the message boards also provide "insiders" a platform to anonymously share with the fans the "true" events without experiencing any negative repercussions. For instance, during a football practice the media members witnessed two key players from a prominent football school, get into a fight. The coach reminded the members of the media that reporting what happened during practice could result in losing practice observation privileges. Although there was no reporting of the incident in the following day's newspapers, this event was relayed on online community message boards within hours of its occurrence [Layden 2003].

There has been limited attention paid to rumors by social scientists in general and IS researchers in particular [Bordia and Rosnow 1998]. Most of the work in rumor mongering has either focused on conceptualizing the nature of rumor from the sociological and psychological perspectives or examining the impacts of the four conditions (uncertainty, anxiety, credulity, and topical importance) in generating and transmission of rumors [Rosnow 1988]. This study's objective is not to delve into the patterns and flows of rumor mongering but rather to compare motivational and normative factors influencing posters and lurkers.

This study focuses on examining the impacts of the motivational and social influences on sharing behaviors which could help explain the driving forces behind sharing content with others in an online environment where tangible rewards for sharing are at best marginal. While there are a number of factors that can be studied in order to understand sharing information and rumor behaviors, motivation is very central in understanding what drives or stimulates some individuals (such as posters as compared to lurkers) to share within the recreational online community where sharing is voluntary and tangible returns are less likely. Therefore, as a starting point, we have selected a parsimonious set of factors emphasized within a more general knowledge sharing literature. These influences not only allow us to explore the differential magnitude of impact of these factors on sharing different types of content, such as information versus rumor, but also allow us to compare whether or not these factors equally influence sharing desires of posters and lurkers. More specifically, we focus on two forms of motivators that have received attention in MIS literature, extrinsic and intrinsic motivation, as well as the potential of normative influence to encourage community members to share. The research questions guiding this work are: *What are the key drivers that encourage an online community member's decision to share information and rumors with others? Are these drivers significantly different for a lurker than for a poster?*

III. THEORETICAL MODEL AND HYPOTHESES

We expect that there are both intrinsic and extrinsic motivational factors and normative influences at play when an online community member chooses to share information and rumors with other community members. However, we believe that those factors will affect lurkers differently than posters. Additionally, we expect that there may be different motivations required for sharing information versus sharing rumors. In the following sections, we briefly review intrinsic and extrinsic motivation, emphasizing prior research on motivational influence on sharing behavior, and we develop the hypotheses used for examining the relationships between motivation and sharing in communities.

Information and Rumor Sharing

The act of sharing information through the use of networked technology has long been a staple of MIS research. The Internet allows workers in organizations to share information and knowledge across large geographical

distances with large numbers of peers. Much ongoing research into this subject deals with ways that information sharing can be encouraged, since the technology itself is no guarantee that sharing will occur [Alavi and Leidner 1999]. The common belief that the organization has an ownership stake in the information generated by its employees is considered to be sufficient motivation for information exchange, whether or not sharing actually occurs [Constant et al. 1994 ; Jarvenpaa and Staples 2001]. Pursuant to the goal of encouraging information sharing behavior, researchers have investigated the influence of reward systems [Bock and Kim 2002 ; Bock et al. 2005], establishing and sustaining prosocial norms for sharing [Constant et al., 1994], coordinating information transfers between agreeable persons [de Vries et al. 2006], among many other possibilities. However, many of these influences are not directly applicable for stimulating information sharing among people outside organizational boundaries, such as sharing on online communities, where individuals are not bound by job duties and responsibilities and sharing is much more voluntary. In online communities, information and knowledge sharing seems to be influenced by different factors.

Recent work by Wasko and Faraj [2000] has uncovered some of the potential motivations that lead members of professional communities of practice to exchange practical knowledge with others, which likely pertains to sharing information. Most of the discussion in these online communities pertains to the profession itself, but the members are under no formal obligation to participate; rather, members are motivated out of a moral obligation. Although there are some tangible rewards for information sharers, sharing behavior is largely the result of wanting to improve the community as a whole. There is also a sense of reciprocity that accompanies information sharing, and members who have not contributed to the community are ignored by many potential information sharers [Wasko and Faraj 2000]. Members of online professional communities are also motivated by social rewards, such as desire to improve one's status and reputation within the profession, which they believe can be attained by sharing knowledge and information with other members [Wasko and Faraj 2005]. Other professionals may be motivated to provide information by a strong culture of organizational citizenship [Brief and Motowidlo 1986]. However, it remains to be seen whether the same rewards apply to other online communities, especially where the act of sharing information is voluntary instead of compulsory.

By comparison, *rumor mongering* received very little attention in the MIS literature. As mentioned earlier, we consider rumor to consist of unsubstantiated information that can vary widely in source credibility. The classic definition put forth by Allport and Postman [1947] is that rumor has a "proposition for belief, passed along from person to person, usually by word of mouth, without secure standards of evidence being present" (p. ix). Rumor is considered different from idle gossip, in that rumors tend to be personally significant to the parties involved, whereas gossip is of much less personal significance [Bordia and DiFonzo 2004]. The reasons for rumor transmission can be numerous. Within an organization, rumors can be communicative methods for sharing or alleviating anxiety, for sense making in times of change, or for predicting the future [Rosnow, 1988]. Rumors can also carry a negative connotation about them, as they can certainly be used to serve the rumormonger's self-interests [Van Bommel 2003]. Not only can they be spread in the traditional face-to-face manner, but the use of computer-mediated communication and online community forums can spread rumors to many more people much more quickly than before.

In fact, the sharing environments that exist within online communities seem to be highly conducive for the transmission of rumors. The ability to participate pseudononymously (posting under an assumed alias) combined with low levels of social presence create a setting of uncertainty and low accountability in which rumors seem to thrive; and any rumor-filled discussions are stored for people to read unobtrusively and relay to others at his or her own leisure [Bordia and DiFonzo 2004]. Despite that, not everyone participates in online rumormongering, and much like criticisms of traditional rumor transmission research have called for [Bordia 1996], there is a need to understand the *motivational involvement* that encourages online community members to share rumors with others. Rosnow [1988] identified four conditions that are necessary for rumor transmission: personal anxiety, general uncertainty, credulity (i.e. plausibility), and topical importance. Each of these four conditions can certainly exist among the members of an online community, particularly one that exists to serve people who share a common profession or interest and would like to exchange information with others. Online communities that are focused on an interest that is in constant flux, and the anxiety and uncertainty that go along with change, are likely more conducive to rumor sharing than those communities that are relatively stagnant. Indeed, the exchange of the latest information and rumors is a top attraction for newcomers to the online community [Norris 2004]. If this is the case, members who share the latest news or rumors are providing a valuable and desired resource to the community. In return, rumors that are eventually deemed to be true can reflect favorably on the rumormonger [Rosnow 1974], especially those rumors that give the monger the appearance of being an expert [Bordia and Rosnow 1998]. Much like the status building and reputation capital gains Jeppesen and Frederiksen [2006] suggest should occur when online community members share his or her unique innovations with other community members, rumors that signal the sharer has a unique inside connection can provide similar rewards, especially if the rumor proves to be accurate.

In order to examine the motivations behind information sharing and rumormongering within online communities of interest, we turned to the Self-Determination Theory (SDT) developed by Deci and Ryan. SDT concerns itself with both autonomous and controlled environments, but its focus on voluntary actions that are taken by individuals with a full range of freedom to behave as they may desire are of interest here. The theory suggests that different types of motivation are prevalent based on the reasons or goals that inspire a certain course of action, with the theory distinguishing between intrinsic motivations, which drive actions that are inherently enjoyable, and extrinsic motivations, which drive actions leading to separable rewards [Ryan and Deci 2000]. These motivations are discussed in more detail in the following section. In terms of autonomous environments, SDT has been used to examine the motivation behind self-behavior in highly emotional situations [Knee et al. 2001 ; 2002] and also in situations in which individuals are focused on specific goal attainment [Kasser and Ryan 1993 ; Wong 2000]. In addition to intrinsic and extrinsic motivations, the community-building and resource-sharing aspect of the current study invoked the examination of normative influences driving sharing behavior. Normative influence has long been associated with the models of behavioral intentions [Fishbein and Ajzen 1975], and it has been identified with helping and sharing behavior by individuals when reinforced through social comparison with others' behavior [Bendapudi et al. 1996 ; Cialdini et al. 1990], the very activity that seems to be in play within online communities of interest. We also discuss normative influence in more detail in the following section.

Intrinsic Motivation

Intrinsic motivation has previously been defined as "the doing of an activity for its inherent satisfactions rather than for some separable consequence" [Ryan and Deci 2000; p.56]. Typically, a person who partakes in an activity due to intrinsic motivation finds the activity fun, interesting, and personally gratifying. There are no external rewards like money or publicity involved for doing so; all of the rewards are internally satisfying to the participant. Further, what is intrinsically motivating to one person may not be similarly motivating to another person. Users who report increased states of enjoyment when using a system will have a more positive experience when performing a task than those who do not enjoy it [Agarwal and Karahanna 2000 ; Hess et al. 2005]. People who enjoy using technology and are intrinsically motivated to use it will be more likely to use it again in the future than people who are less intrinsically motivated.

In the case of sharing information in online communities, intrinsically motivated people would find enjoyment in the act of contributing helpful information to the ongoing discussions. At first glance, online discussion forums would seem to be mainly suited for information gathering, such as for finding support groups or for seeking technical advice. However, discussion forums are not only utilitarian for information seekers, but the more interactive and experiential they are, the more likely their users will also find them to be hedonically satisfying [Huang, 2003]. Further, the intrinsic satisfaction achieved from helping others by providing answers to his or her problems has been observed over interorganizational computer networks. Constant, Kiesler, and Sproull [1996] suggest that when people share information with others across networks, it allows them an opportunity to demonstrate self-expression and subsequent self-evaluation; "people's self-reactions to their own response to others serve as principal sources of reward and sanction" (p.405). We believe that sharing information with other people in online communities provide similar opportunities for self-evaluation and will likewise be intrinsically rewarding for those who choose to do so.

H1A: An online community member's intrinsic motivation is positively related to his or her likelihood of sharing information.

Intrinsic motivations should also compel posters to contribute rumors to the community forum as hearsay becomes privy to them, but according to prior rumor research, the motivations should be different from those that encourage the sharing of information. If information sharing in online communities is grounded in the potential enjoyment and satisfaction from helping others, rumormongering would be motivated by a need to reach a state of comfort or exhilaration. Rosnow [1988] describes the psychology behind the transmission of both distressing and wishful rumors. Passing along rumors that are disturbing to the sharer and are likely disturbing to the recipients seems to be done out of a need to alleviate anxieties or discomfort. On the other hand, sharing rumors that are comforting to the group is likely an attempt to confirm the good news, validating any wishful thinking that has occurred. Finally, Kimmel [2004] states that rumor transmission can hold a great deal of entertainment value for the monger, especially when relaying rumors that have little credibility and are just viewed as amusing subjects to talk about. Where helping others by sharing information offers a chance for altruism and self-satisfaction, sharing rumors with others provides mongers with chances for validation, reducing anxiety, and diversion.

H1B: An online community member's intrinsic motivation is positively related to his or her likelihood of sharing rumors.

Extrinsic Motivation

Ryan and Deci [2000] define extrinsic motivation as "a construct that pertains whenever an activity is done in order to attain some separable outcome" (p.60). Organizational research usually views extrinsic motivators as taking the form of financial compensation, but they can also include perceptual enhancements to one's status and earning recognition from others [Amabile et al. 1994 ; Ko et al. 2005]. These rewards are regarded as "social capital," which are intangible but nonetheless provide valuable network-related benefits [Portes 1998], and gives rise to colloquial expressions like "giving credit where credit is due." Such rewards have long been considered to be efficient motivators, such as in the case of "status competitions," in which individuals seek to gain approval from management by outperforming peers at achieving organizational goals [Lazega and Pattison 2001]. In some studies investigating the motivation for individuals to share knowledge within organizations, extrinsic motivation is viewed solely as an organizational demand and not as an autonomous choice for the knowledge holder [Kwok and Gao 2005]. Through either subtle or overt methods, the individual shares knowledge as a mandatory part of his job duties, gaining rewards for compliance or receiving punishments for non-compliance. However, self-determination theory differentiates that sort of mandatory extrinsic motivation from three other types of extrinsic motivations [Ryan and Deci 2000]. According to the theory, extrinsic motivations can range from the slightly more autonomous *introjection*, which involves alleviating internal anxieties and pressure to perform, to the completely autonomous forms of *identification* and *integrated regulation*. These types typically involve the individual choosing to engage in an activity if said activity is perceived to help avoid feelings of guilt that might occur from not performing the activity, to boost personal self-esteem and pride, or to aid in reaching another related goal. The two autonomous forms of extrinsic motivation are more closely aligned to the voluntary contribution of rumors and information that is the focus of this study.

Unlike professional communities, posters on most recreational message boards are allowed to contribute under a pseudonym, in order to preserve his or her own private identities if they desire. Yet, research suggests that posters care about the reputation and status of his or her online identities within the community. The semi-anonymous environment can allow posters to manage his or her self-presentation and present idealized versions of themselves, even among other anonymous community members who are possibly engaging in similar impression management [Ellison et al. 2006 ; Schlenker and Pontari 2000]. The pseudonyms become the main way to identify and refer to other community members, and over time, become strongly connected to the person "behind the computer." Whether or not a community member's reputation can be explicitly displayed and used for direct comparison with other members [Lin et al. 2006], online reputations are closely guarded and developed. One study [Joinson and Dietz-Uhler 2002] illustrated how strong this connection can become, as a community member invented by a poster and later reported to have been killed resulted in a prodigious outpouring of emotion from the rest of the community (and later outrage after the ruse was revealed). Real posters who value his or her online identities will seek ways to further cultivate and manage his or her associated reputation and status, and this could include sharing information and rumors with other members, providing something of further value to the community.

Knowledge management research has previously noted the influence of extrinsic rewards on both attitudes to share knowledge and the decision to share knowledge with others. In a study of workers' motivations to share knowledge, Bock et al. [2005] found that the desire to gain extrinsic rewards, such as financial inducements and points toward promotion, actually hinder encouragement to share knowledge with co-workers. Whether the blame can be placed on the extrinsic rewards overshadowing any perceived intrinsic benefits from knowledge sharing [Eisenberger and Cameron 1996], or whether the extrinsic rewards for sharing were not perceived as worthwhile or appropriate, the rewards for participation can have the opposite effect on potential knowledge sharers than is desired. On the other hand, online merchants like Amazon.com and eBay.com reward people who post to their recommendation systems and feedback forums with status and reputation-based rankings, which seems to be a practical method for encouraging potential reviewers to post. While not monetary in nature, being publicly acknowledged as a "top 50 reviewer" seems to provide extrinsic motivation for sharing information about products online.

H2A: An online community member's extrinsic motivation is positively related to his or her likelihood of sharing information.

Sharing rumors may also be motivated by extrinsic concerns but could be of a different nature than those motivating information sharing. There may be monetary rewards at stake. A rumormonger with the intent to deceive may be able to sway community opinion about a topic in his favor, or even gain financially from it. Knowing that sharing stock tips online and in trade journals in the form of "whisper forecasts" can predict future stock prices, Van Bommel [2003] found that rumormongers are able to cheat by spreading false information about a stock and trading on it. The extrinsic rewards for sharing rumors need not be solely financial, however. One might expect the rumormonger to derive the same perceived benefits that an information sharer receives, including improved status in the community and earning the respect from those who receive the rumor. According to the resource theory, the more scarce the reliable information surrounding an ambiguous event is, the more valuable even hearsay becomes

[Rosnow, 1974]. The previously-unknown "breaking news" associated with the rumor could provide a boost in status for the rumormonger, especially should the rumor turn out to be true. Rewards like status and image enhancement match what Schiffman and Kanuk [1994] identified as motives for knowledgeable consumers to share his or her unique accounts with others, as it gives them a chance to demonstrate one's expertise, gain attention and notoriety, and to generally show off.

Rumors that are not readily available elsewhere should be perceived as valuable contributions to online community members. Much like sharing information, rumormongering can also present an opportunity for the sharer to put his expertise and inside connections on display. We expect passing along rumors can bring the sharer extrinsic rewards, like improved reputation and status in the community and respect from other community members, motivating them to share.

H2B: An online community member's extrinsic motivation is positively related to his or her likelihood of sharing rumors.

Normative Influence

A third potential motivation to share information and rumors with other community members does not have as much to do with current intrinsic and extrinsic rewards as much as it relates to the normative influence of the other members, particularly those who do post information and rumors. Specifically, we refer to the *normative influence* existing within the community to compel members to share with other members. The descriptive form of normative influence is succinctly explained by Cialdini and colleagues [1990]: "If everyone is doing it, it must be a sensible thing to do" (p.1015). This type of influence holds no bearing on what morally or ethically ought to be done, but instead on what is done by people, based on the behavior of referent others. Normative influence seems to have even more of an effect on behavior depending on who is setting the norm. According to the social identity theory of leadership, there are often prototypical members of a group that emerge as leaders and have a large influence on the norms and behaviors of other group members [Hogg and Reid 2006]. These leaders typify the prototype member, and due to his or her status and influence, are often looked to by community members for normative cues for desirable behavior. Likewise, leaders are able to impose their wills on lower-ranking members because of his or her status, especially when enforcing group norms. Prior research has shown that online communities are populated with some central members who have built relatively large stores of social capital, and these members are most influential in sustaining the community through his or her own posted contributions [Wasko and Faraj 2005]. Even in communities in which there resides a significant number of free riders, a critical mass of resourceful leaders can influence other group members to be good citizens and contribute to the common good through his or her actions [Macy 1990].

Work in the consumer research field has shown that people who are active online have his or her communication motivated by the products and content other influential people have previously developed and communicated. Schau and Gilly [2003] found that most of the respondents to their interviews of personal Web site developers look to others' Web sites for desirable ideas and content to use on their own sites. Appropriating concepts seen on Web sites they desire is seen as being motivated by a need to improve one's online self-presentation. Similarly, Muniz and O'Guinn [2001] relate that consumers who are drawn to an online community focused on a particular product brand often find that it is important to prove they are "true believers" of the brand, as longstanding community members can impose their will through the community status hierarchy. Community members can often find themselves communicating their qualifications as a way to legitimize their membership and make a connection to the high-ranking members.

In the case of online communities, sharing information and rumors are likely seen as being prototypical, desirable behavior. Given a personal attachment to the online community, the power of normative influences on a member's desire to share may be quite strong. According to social norm research, community members should be inclined to share with others if sharing will confer desired benefits, if sharers strongly identify with the community and its goals, and if the act helps sharers define themselves within the community [Lapinski and Rimal 2005]. This more closely follows the "descriptive form" of normative influence [Cialdini et al. 1990], which is based on popular, approved behavior within a community rather than the sanction-based injunctive form of the influence ("what ought to be done") [Park and Smith 2007]. One should not automatically assume that community norms always encourage sharing behavior; there well may be online communities in which new members are intimidated as a rite of initiation. However, we expect that, if members perceive sharing information and rumors as being popular (and even admirable) behavior, performed by popular community members, they would likely choose to engage in that behavior themselves and to be similarly admired by others, while increasing or furthering solidifying their standing within the community.

H3A: An online community member's normative influence is positively related to his or her likelihood of sharing information.

H3B: An online community member's normative influence is positively related to his or her likelihood of sharing rumors.

Figure 1. Research Model

The six hypotheses representing the expected relationships between extrinsic motivation, intrinsic motivation, normative influences, and sharing information and rumors are illustrated in Figure 1. In formalizing our hypotheses, we believe that it is entirely probable that the different motivations and influences would have different behavioral effects on posters and lurkers. Clearly, posters have already chosen to share with the community at least once in the past, whereas lurkers have not made the same choice to share, so behaviorally, there is a difference at the outset. But psychologically, prior research gives us reason to believe that the three independent factors in the research model will be of differing importance to lurkers and posters. As recent work by Ridings, Gefen, and Arinze [2006] indicates, lurkers do not have the same willingness to actively contribute to the community that posters do, and it may be for reasons of distrust or a distaste for social bonding. Ridings and colleagues surmise that a person's trust in the benevolence of fellow community members is strongly attached to motivation to share. In another study exploring lurker and poster attitudes, Preece et al. [2004] found several significant differences between the two types of community members. First, lurkers reported that they were less enthusiastic about the expected benefits of community membership, while posters were more likely to report they enjoyed the benefits of membership and were satisfied that their needs are being met. While it is not clear what those perceived benefits and needs are, these findings hint that posters would be more intrinsically motivated to share than lurkers are. Extrinsically, posters respected other posters more than lurkers respected posters, so it is likely that lurkers do not have the sense of reputation and status-building that posters do. Finally, posters may be more normatively influenced to share as well, as Preece and colleagues found that, although lurkers do consider themselves to be full community members, posters feel a stronger sense of membership. Given these differences in attitudes between lurkers and posters, we tested the research model and hypotheses above for both types of members separately.

IV. METHODS

In order to study the hypothesized relationships between the types of motivations and the content shared by people, we conducted a survey of community members belonging to an online discussion forum that are free to post and share information and rumors as described above. We solicited and gained approval to conduct the survey from the administrators of a Web site devoted to a community of sports fans of the local university's athletic programs. The Web site is available to anyone who registers (at no cost), and at any one time there are several thousands of members. It is impossible to say with certainty what percentage of members actually post to the Web site discussion forum, but during particular sports seasons and recruiting periods, many hundreds of posts may be published daily.

The survey was hosted on an external Web site, and it was made available to all members of the community. The Web site administrators encouraged both posters and lurkers to participate. There were no incentives offered for their participation. After one week of availability, the survey was closed with 651 community members having responded. Unfortunately, a great deal of attrition occurred as respondents could exit the survey at any time, but there were 471 usable responses which were included in the data analysis. Of the completed surveys, 280 were from people classified as "posters," or people who had posted at least one message to the community forum since becoming members. These subjects reported posting an average of 3.29 times per week, with a standard deviation

Communications of the Association for Information Systems

of 6.94 posts. The remaining 191 responses were from "lurkers," who were defined as people who had never posted to the forum. Ninety-two percent of the completed surveys were from males, and the average age of respondents was 38.3 years.

Measures

Items used for the motivation and influence constructs, as well as their factor loadings, are presented in Table 1. Extrinsic motivation was assessed using the items relating to reputation and status that were developed by Constant et al. [1996] and subsequently adapted by Wasko and Faraj [2005] in a study of knowledge sharing in professional online communities. Because there is no possibility for financial rewards for contributing to the community forum, we did not include any items measuring that as a motivating factor, instead including items related to rewards of social capital. A reliability analysis of the extrinsic motivation construct produced a Cronbach's alpha of .87, which surpasses the standard acceptable value of .7 [Cohen 1988].

The measure for intrinsic motivation consisted of the interest-enjoyment items taken from the Intrinsic Motivation Inventory (IMI). While the entire inventory assesses such perceptions as the respondent's competence, locus of control, the effort expended, and pressure and tension felt while performing the task, the seven items that compose the interest-enjoyment construct are considered to be the true measure of intrinsic motivation. In fact, conceptual and statistical analyses of the IMI suggest that the different subscales are not concomitants and are instead causal in nature, and that theoretically, the emotional response that most researchers wish to measure is best represented by the interest-enjoyment measure [Deci 1987 ; Markland and Hardy 1997]. Six of the seven original interest-enjoyment items were included in the analysis. The seventh item, "While I am sharing, I think about how much I enjoy it," cross-loaded with the normative influence factor, and with its own loading on the intrinsic motivation factor at .387, it was dropped from the analysis. The reliability of the remaining six items was satisfactory, resulting in a Cronbach's alpha of .91.

Table 1. Items and Factor Loadings

Item		Intrinsic	Extrinsic	Normative
I enjoy sharing very much.		**.83**	.23	.07
Sharing is fun to do.		**.85**	.23	.11
Sharing is a boring activity.	*RC*	**.78**	-.07	.18
Sharing does not hold my attention at all.	*RC*	**.78**	-.08	.14
I would describe sharing as very interesting.		**.78**	.25	.02
I think sharing is quite enjoyable.		**.86**	.22	.03
I earn respect from others by sharing.		.10	**.79**	.18
I feel sharing improves my status in the community.		.10	**.86**	.18
I share to improve my reputation in the community.		.04	**.88**	.19
I appreciate people who share on the forum.		.19	.16	**.90**
I admire people who share on the forum.		.09	.35	**.84**

RC = reverse coded item.

We measured normative influence using two exploratory items, not the five-to-six item traditional measure, which was not considered appropriate given the online, psuedoanonymous context. Instead, we constructed items that conveyed the importance of normative influence in this type of online community. We believed members who provide valuable resources (information and breaking rumors) to the community would be viewed by respondents as prototypical, and that an appreciation of prototypical member behavior would have a normative influence one's own decision to share. The two items for normative influence, displayed in Table 1, showed satisfactory reliability (α = .84).

The dependent variables, sharing information and sharing rumors, were also measured on the questionnaire. The items asked how likely the respondent would share new information (and in the second item, rumors) about the university athletic program should he or she come into possession of it: "If I have information about (the university's athletic program), I would consider posting it on (the discussion forum)," and "If I hear rumors or hearsay about (the

university's athletic program), I would consider posting it on (the discussion forum)." The responses for both were assessed using a seven-point Likert scale, anchored by "strongly disagree" and "strongly agree." Single-item measures are appropriate if the construct being measured is narrow and unambiguous to subjects (Sackett and Larson 1990). To provide context to the items, we explained that sharing information could take the form of updating scores from ongoing games, providing updates to players' injury status, sharing confirmed future schedules for the university's sports teams, or other factual responses to another member's questions. Rumors could involve speculating about future game lineups, prospective recruits to the university teams, potential coaching changes and the like, and in a further effort to differentiate sharing rumors from information, rumors were associated with the more colloquial term "hearsay" on the survey.

Table 2. Means, Standard Deviations, Reliabilities, Inter-Construct Correlations, and Square Roots of AVE Values (Includes Both Posters and Lurkers, n = 471)

Factor	Items	Range	Mean	Stan. Dev.	Cronbach's α	Intrinsic	Extrinsic	Normative	InfoShring
Intrinsic	6	1-7	4.52	1.35	.91	**.795**			
Extrinsic	3	1-7	2.71	1.38	.87	.330	**.845**		
Normative	2	1-7	3.67	1.55	.84	.358	.474	**.865**	
InfoSharing	1	1-7	5.27	1.36	--	.330	.158	.154	--
RumorMng	1	1-7	3.57	1.73	--	.281	.453	.459	.347

Figures in bold are square roots of the average variance extracted by the factor.

The descriptive statistics and intercorrelations for the three independent variables are displayed in Table 2. In addition to showing satisfactory reliability and convergent validity, the constructs showed appropriate discriminant validity, judging from the AVE values being higher than each of the constructs' correlations with the other two constructs. Finally, we conducted a wave analysis to test that data for the possibility of nonresponse bias [Hsieh, Rai, and Keil 2008]. Early survey respondents can sometimes provide drastically different than later respondents, so we compared the individuals who responded the first day of the survey with those who responded during the last three days of the week. T-tests of the three independent variables and the two dependent variables revealed no significant differences between the early and late respondents, suggesting there was minimal nonresponse bias.

Results

Analysis of the research model and the six hypotheses was performed using AMOS 4.0 for structural equation modeling (SEM) with maximum likelihood estimation. In order to ascertain how the hypothesized relationships occur among posters and among lurkers, we split the subjects into one of the two categories. Thus, two separate models were tested using a bootstrapping procedure, with 100 independent samples supplied for each. Figure 2 shows the evaluated structural models. The chi-square statistics for each model provide a test of the null hypothesis that the reproduced covariance matrix has the specified model structure, i.e., that the model "fits the data." The goodness of fit indices statistics, i.e., the comparative fit index or CFI (Bentler 1989) may range in value from 0 to 1, where 0 represents the goodness of fit associated with a "null" hypothesis model (one specifying that all variables are uncorrelated), and 1 represents that goodness of fit associated with a saturated model (a model with 0 degrees of freedom that perfectly reproduces the original covariance model), and a CFI greater than 0.8 is preferred. Finally, the root mean square error of approximation (or RMSEA) is computed using the non-centrality parameter and is commonly used to estimate the misfit of the model, with evidence of misfit considered to be an RMSEA of 0.10 or greater (Browne and Cudeck 1993). The model representing posters' motivations displayed appropriate goodness-of-fit (χ^2 = 261.58, *df*=83, p<0.01; CFI = 0.95; RMSEA = 0.08), as did the lurker model (χ^2 = 229.97, *df*=83, p<0.01; CFI = 0.93; RMSEA = 0.08).

Using a predetermined α of .05 to signify statistically significant effects for two-tailed testing, there was ample support found for Hypotheses 2B, 3A, and 3B, as those relationships were found to be significant in both models. In other words, extrinsic motivation was found to be a significant influence in the decision to share rumors, and normative influence was found to be a significant influence when sharing information and rumors for both posters and lurkers. Hypotheses 1A and 1B were significant only for posters, and Hypothesis 2A was not supported in either case. This provided evidence that intrinsic motivation is a factor in posters' decisions to share, but not for lurkers. Neither lurkers nor posters seem to be extrinsically motivated to share information. The models explained 26 percent of the variance in sharing information and 42 percent of the variance in sharing rumors for posters, and only 4 percent of the variance in sharing information and 45 percent of the variance in sharing rumors for lurkers.

V. DISCUSSION AND IMPLICATIONS

Overall, lurkers and posters seem to somewhat differ in the structure of factors motivating their sharing information and rumor behaviors. More specifically, the results reveal that the posters' likelihood of sharing information and rumors are shaped collectively by all three factors, i.e., intrinsic, extrinsic, and normative, while lurkers are primarily driven by extrinsic and normative influences. Therefore, it appears that the significant positive impact of intrinsic motivation on sharing is the most critical relationship which differentiates poster from the lurkers. A post hoc analysis uncovered that the magnitude to which the posters' and lurkers' motivational and normative factors impact sharing behaviors differ to a greater extent for rumor sharing than for information sharing (see Table 3). More specifically, the posters' rumor sharing behaviors are impacted by intrinsic motivation and normative influences to a significantly greater extent than for the lurkers (Intrinsic: $t=4.35$, $p<0.001$; Normative: $t=4.33$, $p<0.001$); whereas, the lurkers' rumor sharing behaviors seem to be driven by extrinsic motivations to a greater degree than for the posters (Extrinsic: $t=-6.40$, $p<0.001$). On the other hand, there is no significant difference in the extent to which extrinsic ($t=1.28$, ns) and normative ($t=0.87$, ns) factors impact the posters' and lurkers' information sharing behaviors; however, they do differ in their intrinsic motivation's impact on information sharing ($t=6.33$, $p<0.001$).

Figure 2. SEM Results

Table 3. Motivational Differences between Posters and Lurkers

Motivational Effect	Beta-value		t	Eta squared
	Posters	Lurkers		
Intrinsic – Share Info	.58	.07	6.32 *	.08
Intrinsic – Share Rumors	.38	.04	4.35 *	.04
Extrinsic – Share Info	.04	-.06	1.28	.003
Extrinsic – Share Rumors	.14	.73	-6.39 *	.08
Normative – Share Info	.21	.13	.86	.002
Normative – Share Rumors	.77	.31	4.32 *	.04

* - significant at .05 level

Although people were likely attracted to the site because of the shared interest in its subject matter, we know that the respondents in this study were more interested in the community for its capacity for information gathering than for meeting other people sharing the interest. A combined 88 percent of the subjects responded that their main reason for visiting the Web site was for gathering information and rumors about the athletic program, as opposed to socializing, "trash talking" other universities and their sports programs, or merely as a way to spend free time. The Web site administrator verified this anecdotally. The two most-visited days in the Web site's history involved high-profile, but largely ambiguous, situations. One involved the possibility of the university's longstanding football coach interviewing for (and eventually taking) a similar position at another university, and the other situation involved discussion around the nation's top high school football recruit's decision to enroll at either the university or one of its main rivals. According to the Web site administrator, there was no shortage of rumors being posted in either case.

Intrinsic Motivation: Although intrinsic motivation is a significant predictor of posters' sharing behaviors, it failed to significantly impact lurkers' attitudes toward sharing. Intrinsic motivation assessed participants' subjective experience, i.e., enjoyment and interest, with regard to sharing. Posters reported that contributing content to the forum is enjoyable, satisfying, attention-holding, and overall fun, and this appears to influence both sharing information and sharing rumors. On the other hand, lurkers' anticipation of the intrinsic rewards did not significantly influence their decisions to participate in information sharing or rumormongering. One explanation for this finding is that lurkers simply do not see the possible enjoyment and satisfaction in sharing with the community until they try it. It is only through the act of posting can a person truly experience the rewards associated with this process. Venkatesh [1999] speculated that achieving high levels of intrinsic motivation is likely to lead to sustained usage of technology, but the system user must first employ the system in order to enjoy it. It is possible that lurkers must first post in order to enjoy sharing with others. We did not attempt to measure if lurkers have additional online identities on other Web sites, so it is also possible that lurkers' intrinsic motivation varies from community to community, especially if they have actually posted within those other communities. On the other hand, posters seem to continually return to the community forum due to the personal satisfaction they receive from exchanging information and rumors with others. In fact, the results indicate that posters might be more intrinsically motivated to share information than to share rumors, an attitude that might result from the larger number of informational posts than rumor-filled posts on the community forum. By definition, rumors are a rare resource and thus harder for people to attain and share with others. The majority of our posters probably had more experience sharing information than rumors and could identify better with the intrinsic rewards associated with it.

This result, that intrinsic motivation positively impacts a poster's sharing likelihood, is consistent with other studies in the literature. However, this study's findings differ from results reported by Wasko and Faraj [2005], who found that members of online professional communities were not intrinsically motivated to share, surmising that the lack of anonymity offered and the importance of one's reputation weakened the influence of intrinsic motivation to share. This difference could be an artifact of the differences in the methodological approaches used to capture the sharing behaviors (assessing actual posting activity versus self-reports on posting behaviors used in this study). Nonetheless, it is worth noting that although both the community featured in this study and the community in the Wasko and Faraj study are voluntary in terms of participation, they both have varying goals. The involvement observed in the latter study focuses on enhancing one's career whereas involvement in the former is largely a function of one's personal enjoyment and interests. This supports the current study's thesis that online communities are not monolithic entities with congruent goals; therefore, the behaviors observed in one type of an e-community, such as a community of practice, may not be easily generalizable to other types of communities. Therefore, in order to enhance our understanding of the behaviors observed within online communities, future research needs to examine e-communities with diverse settings and objectives.

Extrinsic Motivation: The results indicate that the extrinsic motivation increases the posters and lurkers likelihood of sharing rumors but has no significant effect on their likelihood of sharing generally-accepted information. The respondents perceive that the way to improve one's status in the community and gain the enviable reputation as a knowledgeable source is to produce rumors that most other people, perhaps even the Web site administrators, may not be aware of. Within the e-community examined in this study, simply being helpful and providing information to other members is not enough to boost status or reputation, at least not in the respondents' eyes. This finding corresponds to the social capital theorizing by Lin [2001], who suggests that social transactions can be asymmetrical, in that some assets exchanged within the community may not be as easily produced and contributed by many members who seek to reciprocate. This would be the case with rumormongering, which involves the exchange of content that is initially unavailable to people other than insiders. Lin suggests that the asymmetry leads to a buildup of social credit for the asset provider, leaving the asset takers with a social debt. In the context of this study, information exchange between community members may be more easily reciprocated (with asset takers easily expunging the debt), but the likelihood of reciprocating rumor exchange is more difficult, thus requiring the repayment of the debt in another way. Often, the debtors repay by publicly acknowledging the value of the social transaction, spreading the asset donor's reputation throughout the network [Lin 2001]. In doing so, the donor is

repaid by the community as a whole [Portes 1998]. This seems to be the case for the community members engaged in rumormongering in this study.

Still, the role of extrinsic motivation within the context of sharing behaviors is unresolved [Huber 2001]. For instance, studies of professional e-community of practice found that extrinsic motivation, i.e., reputation, to be a significant predictor of knowledge sharing behavior [Wasko and Faraj 2005]. As discussed in the previous section, the impact of extrinsic motivation on sharing behavior is different in this study than what is found in studies examining the community of practice. Moreover, the role of rumors as a critical asset is applicable to recreational community, but cannot be generalized to all the online communities. These results confirms our assertion that online communities are not monolithic entities with congruent goals and therefore, the behaviors observed in one type of an e-community, such as a community of practice, may not be easily generalizable to other types of communities. Within the organizational boundaries, where sharing information could be considered part of one's job duties and commitment to the organization [Constant et al. 1994], extrinsic motivation's impact on knowledge sharing has varied from negative [Bock et al. 2005], non-significant [Ko et al. 2005], to positive [Kankanhalli et al. 2005] depending on the context of the study. It appears the impact of extrinsic motivation is complex and situational in nature, which again reinforces the need for examining the sharing behaviors in various e-contexts.

The finding that the value of rumormongering is apparent to both posters and lurkers indicates the power of perception with regard to contributing unique accounts through rumor to the community. All members seem to be of the same opinion that breaking previously unknown "news" is the best way to achieve personal status and reputation enhancements. Nothing else seems to leave a more lasting impression among community members. Of course, being associated with a rumor that is proven false may be an effective way to undoing those enhancements [Kimmel 2004], but that has yet to be studied in online communities. Moreover, it is conceivable that rumor sharing is more salient within certain online communities, such as sports message boards, where its speculative content has a value. However, rumormongering could be rather detrimental in other e-communities, such a community of practice, where content accuracy is crucial. Therefore, future research needs to further examine the rumor sharing behaviors within various e-communities.

Finally, it should be noted that information and rumors that are gleaned from online communities like the community examined in this study can provide extrinsic benefits to members when offline. The literature on sports team identification suggests that one's association with a particular sports team often produces unique social connections and reduces alienation in the workplace [Wann 2006]. Sports can provide a topic of discussion that allows people occupying different strata within the company to communicate meaningfully with each other, to the point where individuals with shared interests specifically seek each other out. As Melnick [1993] explains, "When strangers feel that they can be of service to one another, they're more likely to interact... Some fans are 'walking encyclopedias' of sports trivia and esoteria who are only too willing to share their information" [p. 50]. The respondents in this study may well engage in such activities with coworkers, benefitting extrinsically outside the online community.

Table 4. Means, Standard Deviations (in parentheses), and Differences of Measures between Lurkers and Posters

Factor / Measure	Lurkers (n = 191)	Posters (n = 280)	F (sig.)
Intrinsic	4.44 (1.56)	4.56 (1.17)	.998 (p = .32)
Extrinsic	2.67 (1.40)	2.74 (1.36)	.227 (p = .63)
Normative	3.57 (1.57)	3.74 (1.53)	1.38 (p = .24)
Sharing Information	5.62 (1.02)	5.03 (1.49)	22.73 (p < .000)
Sharing Rumors	2.87 (1.68)	3.96 (1.66)	47.74 (p < .000)

Normative Influences: Normative influence significantly impacts both the posters' and lurkers' inclination to share information and rumors. As the means for the normative influence measure in Table 4 indicate, both groups of community members appreciate and even admire the members who share. This attitude is important to the survival and growth of a community. Without a critical mass of community members that share useful and compelling content, the community stands the chance of stagnating and even going extinct [Morris and Ogan 1996 ; Preece et al. 2004]. This recognition, that content development which sustains the community is dependent upon the members who frequently share information and rumors, puts social pressure on the other members to contribute. However this normative pressure is not enough to bring about a behavioral change among lurkers. Because lurkers do not make the decision to share behaviorally, it appears that normative influence by itself is inadequate to compel them to post. It would be valuable to think about ways to apply and heighten normative influences on the community

members. One way to do that would be to reward and showcase the contribution of active members. For instance, the active members who frequently post rumors before that content becomes news could be highlighted by displaying poster ratings or even placing different color stars in their online profiles. While playing upon community members' extrinsic motivations, such graphic representations could simultaneously serve to encourage and reinforce community norms for sharing. Lurkers may still need to be reassured that their community peers are competent and to believe that the community members do share more than just a common interest in the topic of discussion; community members may have very similar life experiences and backgrounds, and by witnessing these similar people willingly share with the community, lurkers may become more trusting and become influenced to do likewise [Leimeister et al. 2005]. Interestingly, the mean for sharing information was higher for lurkers than it was for posters, which could suggest that lurkers would consider sharing general information before attempting the more provocative rumormongering, and that dovetails with the problem with initially trusting other community members that seems to confront lurkers [Ridings et al. 2006]. Overall, the results suggest that either normative influence may merely be a necessary, yet insufficient, condition for sharing or its association with the likelihood to share needs to be much stronger. Future research should examine the magnitude of this relationship in order to fully understand its role on sharing behaviors.

VI. LIMITATIONS

This study is not without limitations. One chief limitation is derived from the manner in which we collected data from the subjects. Much like the earlier research done on sharing by Constant and colleagues [1994 ; 1996], this study focused on perceived attitudes and motivations, thus we did not measure actual sharing behavior. We were not granted access to any administrative rights to this particular online community, so we had no way of reconciling subjects (whose online identities remained unknown to us) with their actual participation in the community. We thus relied on self-report responses to test the hypothesized relationships. Moreover, the subjects responded to single-item measures for both information sharing and rumormongering, but both items could be considered hypothetical since there are no guarantees each subject will eventually come into possession of unique information or rumors to share. However, the items reflected the research questions driving this research, namely the impact of motivational influences on a person's willingness to share in an online community of interest. Actual behavioral data would be valuable for future research that investigates the amount of information and rumor sharing that does take place in these communities. Although matching the posters' perceptual responses (captured via a survey) with their actual postings would mitigate the concerns associated with the mono-method bias, that approach would not allow us to fully address this study's research questions which entail a comparative analysis of the lurkers' and posters' motivational drives. A related limitation involves the classification of our subjects. We classified all subjects who responded affirmatively to the survey question, "Have you ever posted to the community message board?" as posters, with those answering negatively as lurkers. Unlike other recent studies [Ridings et al. 2006], we made no distinction between those who have posted only one time and those who have posted much more frequently. The variance for posting frequency was not spread widely among respondents, as 90 percent of the posters reported posting once or less per day. However, the results of this study should not be appraised without acknowledging this classification of all posters.

Another limitation of this study is that this study surveyed the members of only one online community, it being a community centered around one intercollegiate sports program, which limits the generalizability of our results. Our research differs from prior studies using professional communities of practice, in that this study involved a community sharing information of a primarily hedonic nature, and care should be taken not to extrapolate the findings to an organizational or professional forum. Our posters are identified by an alias, and lurkers were not required to identify themselves at all; however, this limitation also identifies an avenue for future research, namely exploring the difference in motivations between identified and anonymous community members. Unlike prior research on professional communities which saw little in the way of intrinsic motivation for members to post [Wasko and Faraj 2005], the posters in this study were highly influenced by intrinsic factors. Posters seemed to share information and rumors merely "for the love of the game" more than for extrinsic reasons, whereas lurkers, who were not motivated intrinsically to share, were not compelled to post and chose to remain in an observational, information seeking role, and seemed only likely to post rumors in the future for the potential notoriety that might result for doing so. Future research could expand on the positive/negative valence of the rumors that are contributed and the intrinsic rewards resulting from that [Heath 1996], which we did not explore in this study.

Additional attention should also be given to technological properties that may serve to either encourage or discourage contributions to the forum. The use of aliases, for instance, is one enabler that online communities can offer to encourage sharing possible inflammatory content like rumors. However, sites that allow too much unfounded content may run the risk of driving away members, so system attributes can be utilized to find a healthy medium. For example, as a way to provide a manner of accountability to online communities, many administrators require that members must initially create user accounts before submitting content to the forum. For some lurkers, the act of registering with the community, even under an alias, may discourage them from posting. The particular

online community used in this study required all members, even lurkers, to register before being able to even access the forum, so the registration barrier did not moderate our results. Further, our community members who have enabled cookie acceptance on their Web browsers have no need to log in to the community in the future. However, we do acknowledge that other online communities differ in registration and log-in procedures, so future research focusing on these system attributes and their potential impact on motivation to share.

We acknowledge that the content posted and shared on the online discussion boards may not always fall neatly into the two content types (information and rumor) that are examined in this study. Additionally, the two content types themselves are multifaceted, so depending on the community and the context of the discussion, the content that is posted can vary widely. In a study such as this, it would be impossible to query subjects on every single type of information or rumor that could possibly be posted. However, information and rumors are critical fuel for driving certain online communities such as the sports discussion boards and therefore, it is valuable to examine the motivators for sharing such content in general. This study uncovers and empirically demonstrates that rumor serves as a scarce and valuable resource that can help with the creation and sustenance of a recreational online community, and our findings suggest that rumor should be viewed differently from other types of posted content. To our knowledge, there are no IS studies that have examined and demonstrated the role of rumors in cultivating and maintaining an online community. Future research should extend this research by examining the sharing behaviors of other types of content. Recent work investigating the sharing of music and other copyrighted material within online peer-to-peer networks indicates that a popular resource, even when illegally distributed, will attract people with similar interests and desires, and that there are a number of other people who gladly share content with them [Bhattacharjee et al. 2006]. Efforts to reduce the amount of music piracy could benefit from an exploration of the motivations compelling individuals to participate in P2P file sharing.

Finally, while we believe that this study provides a starting point to the phenomenon of online rumormongering, we also believe that there is much more left to uncover. As online communities become even more prevalent with time, especially as they become more cost-effective for businesses who use them to improve Web site metrics [Bughin and Hagel 2000], the incidence of rumormongering is likely to increase accordingly. Though there is an unfortunate lack of research on online rumormongering, we believe that there are parallels between the virtual world and the physical world with regard to the value of rumors to online communities. Rosnow [1988] studied the nature of rumors in professional environments and places a great deal of importance on management's ability to prevent rumors from running unchecked, and further, advises that managers warn about the destructive consequences of false rumors. In online communities of practice, findings indicate that quality of information is important for maintaining commitment to the community and the reciprocal sharing of high quality information [Wiertz and de Ruyter 2007]. Rumors are likely more appreciated in online communities of interest. Hagel and Armstrong [1997] advise that online community organizers do much like their counterparts in the physical world do in order to attract interest in their clubs and social groups; they should take advantage of people who are "well connected" within an existing information network and are able to provide content of interest to the community, generating a critical "buzz" for the community. In the community we studied, there are people who, at least, claim to be "well connected" to the athletic program and provide rumored information that is unavailable anywhere else. According to the Web site administrators, this type of content seems to be the most popular, driving more page views and longer discussion threads. Though this might not be the case within all online communities of interest, we cannot help but believe it is the case with many. Thus, rumors should be considered to be fundamentally multifaceted and not automatically disruptive or counterproductive. The current scarcity of research on rumormongering in online environments is certainly an area that future research should address. Finally, future studies should focus on other ways that online communities can increase advertising revenue. The addition of content from converted lurkers may be one method, but encouraging community members to support the site's advertisers is another challenge. Future research could help direct administrative efforts toward even more fruitful methods.

VII. CONCLUSION

Despite potential limitations we believe that this paper makes some important contributions. This study extends prior literature by examining sharing behaviors of two types of community members in a different setting than the more commonly examined communities of practice setting. Where prior studies have focused on the psychological factors and perceptions that ultimately discourage sharing behavior, we sought to explore the different motivations that can encourage voluntary sharing. The results of this study broaden our understanding of the factors that shape the sharing behaviors of lurkers and posters within e-communities which have a recreational focus. Lurkers are often reported to be the majority members in an online community, ranging from 50 to 90 percent of the total membership (Mason 1999; Soroka et al. 2003; Katz 2003). The advertising-driven business model that many sites are built on survives on the online community which consists of both posters and lurkers. Given the size and the importance of the lurking community, it is critical that it receives more attention than it has received from the IS community ; therefore, this majority pool of lurkers provides a substantial resource for the recruitment of "new" active members. Yeow and colleagues [2006] conclude that, "lurking as an online social phenomenon is more

complicated and nuanced than previously discussed in the literature" (p. 980). This study takes a small step in that direction and can be used as a building block for future studies focusing on the lurking community.

Moreover, the study provides evidence that posters and lurkers are differently motivated based on the type of content they might be tempted to share, which, to our knowledge, has not been investigated within online communities. This study highlights the need to further investigate rumor-based content, which appears to be a valuable resource in some online communities. We expect that the decision to share with other community members does involve whether general information or unsubstantiated rumor is to be posted, and posters and lurkers seem to differ in the anticipated rewards derived from the decision. While we acknowledge that this one study does not provide a complete view of sharing behaviors of lurkers and posters, the empirically validated model with variables included in this study provides a good starting point for building future studies on this topic.

國立雲林科技大學
99學年度博士班招生考試試題

系所別：資訊管理系
科　目：資訊科技文獻

An Exploratory Cognitive Business Intelligence System

請依據文章內容以中文回答下列問題：

1. 請說明本篇論文的主要論點。(20%)

2. 請說明決策主管如何使用建議的系統進行決策。(20%)

3. 請說明作者所建議方案之主要理論依據。(10%)

End-to-end Web Application Security

請依據文章的內容用中文回答下列問題：

4. 作者為何不認同將安全機制全部依賴伺服器端？(20%)

5. 本文所提出的方法有賴於哪些前提的成立？(10%)

6. 請描述作者所提出來的基本安全政策及動態安全政策。(20%)

國立雲林科技大學
99學年度博士班招生考試試題
系所別：資訊管理系
科　目：資訊科技文獻

An Exploratory Cognitive Business Intelligence System

Li Niu*, Jie Lu§ , Eng Chew§, and Guangquan Zhang§
Faculty of Information Technology, University of Technology, Sydney, Australia
ollieniu@hotmail.com, §{jielu, engchew, zhangg}@it.uts.edu.au

Abstract

An exploratory study of web-based cognitive business intelligence systems (CBIS) is presented in this paper. The underpinning concepts and theories are situation awareness, mental model, and naturalistic decision making (NDM). The CBIS is an extension of the traditional business intelligence system with cognitive orientation. It focuses on developing, enriching, and utilizing the executive's situation awareness, mental models, and other past experience during human-computer interaction, which drives the decision process to approach a naturalistic decision.

1. Introduction

Decision support systems (DSS) are envisioned as "executive mind-support systems" that are able to support decision-making process from human cognitive aspects [1]. Nevertheless the emphasis of today's DSSs falls into either powerful data analysis functionality, or mathematical and statistical models, or efficiency of group communication [2, 3]. Cognitive orientation in DSS remains weak albeit it has long been recognized as an important consideration [1, 4]. This is also the case of business intelligence (BI) systems, a kind of data-driven DSSs, focuing on the manipulation of large volumes of company data in data warehouses.

The notion of cognitive orientation grounds in cognitive psychology, of which situation awareness (SA) and mental model are two important concepts. The decision-maker's cognitive ability (driven by SA and mental models) plays a key role for dealing with unstructured problems with time pressure, uncertainty and high personal stakes [5, 6]. The concepts of SA and mental model form the basis of naturalistic decision making (NMD) models, i.e. recognition-primed decision model (RPD).

The objective of this research is to enhance the analytical functionality of traditional BI systems through extending traditional BI systems on cognitive orientation. We develop a cognitive business intelligence system to support the executive's SA and mental models for better decision making. The CBIS is based on a data warehouse subsystem, a case base, and a mental model base. The decision-making process in the CBIS is based on RPD model.

2. Theoretical fundamentals

Situation awareness (SA) is a cognitive psychology concept. Endsley [5] suggests SA is divided into three levels of mental representations: perception (level 1 SA: perceiving raw information from the environment), comprehension (level 2 SA: understanding perceived information), and projection (level 3 SA: predicting the future status of the environment). The development process of SA is called situation assessment [5]. This process can be enhanced by means of appropriate technologies.

SA is believed to be an essential prerequisite for people's decision making in any complex and dynamic situations. Many incidents or mishaps that resulted from inadequate SA of the operator have been widely examined [5, 6, 7]. Mental models are commonly referred to as deeply held assumptions and beliefs that enable individuals to make inferences and predictions [1, 8]. Mental models are important for decision making through acting as reasoning mechanism and by affecting situation assessment.

In the study of decision making, naturalistic decision making (NDM) has emerged as a new discipline since 1980s [9]. Recognition-primed decision (RPD) model is the prototypical NDM model [10]. The emphasis of the RPD model is situation awareness. When presented in a decision situation, the decision maker will try to recognize the current situation through developing concurrent SA. The recognition results in feasible

goals, important cues, and potential solutions to the situation. An emerged promising course of action is quickly screened for feasibility, and then selected or rejected. If an option is rejected, a second one will be tested, and so forth, until a feasible option is selected. The screening process much more relies on pattern matching and informal reasoning rather than analytical reasoning [10].

From information systems perspective, cognitive orientation has significant implications for enhancing the functionality of traditional BI systems. Traditional BI systems can only partially support executives' management process [11]. A BI system is capable of providing executives with a huge amount of instant data. However, more data does not equal more valuable information [12]. Executives often feel lost when presented with a large body of data concerning decision making. A recent survey, by Economist Intelligence Unit [13], shows 73 per cent of senior managers agree that it is important to have less but more timely data to improve the quality and speed of decision making. This result corresponds to the research result by Sutcliffe and Weber [14] about the knowledge accuracy. Their research implies that having a lot of facts about the company is less important than having a clear and consistent overview picture.

3. System architecture

3.1. Executive

The CBIS is a user-centered information system where the executive (the decision maker) is the central component. The executive is not only a user of the computer system, but also one of the important considerations for the design of other components. On one hand, like other computer-based information systems, the executive behaves as a user during human-computer interaction, e.g. typing texts into or getting feedback from the computer system. On the other hand, the CBIS is based on cognitive orientation that focuses on user-centered implementation.

3.2. Thinking support

Thinking Support module is intended to provide the executive with a set of tools for knowledge management and thinking process support. Think support is made up of five submodules: case base, mental model base, case management, mental model management, and knowledge agent. The knowledge is stored in knowledge base including case base for explicit knowledge and mental model base for tacit knowledge. Case management and mental model management are responsible for acquiring, representing, storing, and retrieving respective knowledge. Knowledge agent conducts knowledge analysis and receives knowledge requests from other modules.

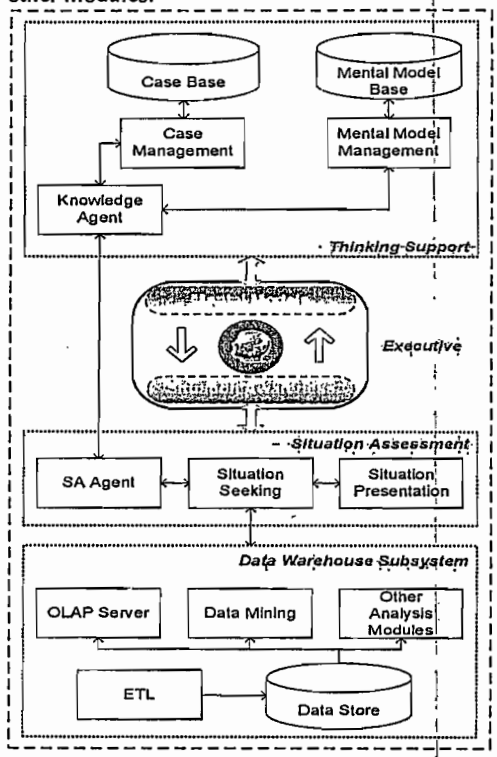

Figure 1 System Architecture

Case base. Cases are explicit knowledge that reflect the results of past problem solving. Cases can be acquired from an individual (e.g. the executive) or a group. In case-based reasoning, several case representation approaches are available, such as textural approach, conversational approach, and structural approach [15]. We adopt attribute-value approach to represent cases in the CBIS.

Mental model base. Mental models can be elicited as the approximate representation of human mental constructs from the executive using cognitive mapping technique [16]. The output of cognitive mapping is cognitive maps. A cognitive map consists of concepts (nodes) and relationships (linkages). A cognitive map reflects the causal relationships between different concepts.

Case/mental model management. The functionality of this module is to acquire, represent, load, retrieve, update, and delete cases/mental models. It provides knowledge workers an interface to manage cases/mental models.

Knowledge agent. Knowledge agent receives knowledge requests from SA agent (a submodule of situation assessment module) and parses, delivers the requests to both case management and mental model management. A knowledge request is the description of the executive's information needs concerning current decision situation. If knowledge agent gets back retrieved results (cases and/or mental models), it filters and integrates them. Knowledge filtering can be carried out automatically or supervised by the executive through a user interface of knowledge agent. Knowledge is retrieved, filtered and integrated in the light of knowledge requests.

3.3. Situation assessment

This module is responsible for aiding the executive to develop SA about current decision situation. In this paper, from information system perspective, situation assessment is regarded as a data processing process during which situation data of interest is retrieved, analyzed, presented, and understood by the executive. Situation assessment is comprised of three submodules: SA agent, situation seeking, and situation representation.

SA Agent. SA agent receives SA inputs of the executive and requests corresponding knowledge from thinking support module. After getting requested knowledge, SA agent integrates SA with knowledge to produce a description of information needs of the executive regarding current situation. The information need is then parsed into mdXML (Multi-dimensional Extensible Markup Language) elements for retrieving situation data from the data warehouse. mdXML is a kind of markup language developed for accessing multiple-dimensional data (cubes). For more details about mdXML, please refer to http://www.xmlforanalysis.com/.

Situation seeking. Situation seeking module is designed to seek data relevant to current decision situation. Situation seeking receives the information need in the form of mdXML element from SA agent and then retrieves situation data from the data warehouse via OLAP server. According to pre-defined business rules, retrieved situation data is either passed to situation representation module or performed further analysis, e.g. data mining. Further analysis is provided by corresponding analysis module in data warehouse subsystem and the analysis result is returned back to situation seeking module and then sent to situation representation module.

Situation representation. This module represents the situation data to the executive. Situation data is represented using data visualization techniques, such as graph, chart, plot.

3.4. Data warehouse subsystem

The data warehouse forms the factual basis on which the decision situation is retrieved, presented and assessed. The data warehouse subsystem is developed based on traditional BI system framework. This subsystem is made up of operational systems, data acquisition, data storage, and data analysis module.

4. The use of the CBIS

The CBIS is a web-based decision-making system with situations as its input and decisions as output. When a situation is presented to the system, the decision process starts from the executive's initial SA about the situation. The initial SA can be obtained in different means, e.g. business meeting. The executive's SA is input into the system and represented as computer information objects. After the CBIS receives the executive's SA input, it retrieves case base and mental model base which closely related to the SA. Cases and mental models are the representation of the past business management experience. They have strong implications to dealing with current decision situation. Retrieved cases, mental models and SA are integrated and parsed into the information needs. The information needs are used to retrieve data warehouse for the seeking of situation data. Situation data is visualized and presented to the executive. The executive perceives information from situation representation and understand it through combing her/his past experience. The executive's cognitive process will eventually produce updated SA richer than the initial SA input. At the end of each interaction cycle (starting from initial SA input and ending at updated SA), the executive will have deeper understanding of the current situation and is more likely to make a good decision. The interaction cycle continues if the executive resubmits her/his SA to the system for richer SA and better decision. Otherwise the executive makes the decision and the interaction loop ends. In the real settings, several factors affect whether a new

interaction cycle starts, such as permitted decision time, the executive's confidence, and stakeholders' opinions.

5. Conclusions

With the attempt to achieve a higher degree of human-computer interaction and make computers to cognitively support humans in decision-making processes, this paper proposes a web-based cognitive business intelligence system. In this system, the related theories and concepts of cognitive psychology and decision making are combined with current BI systems framework. Compared with traditional BI systems, the CBIS shows the three characteristics. (1) Cognitive orientation is a key consideration in the system design. SA and mental models are integrated into the system; (2) the decision process in the CBIS is driven by the executive's cognition and based on the RPD model. A decision is approached by enriching the executive's SA and mental models, rather than a computer's decision suggestion; (3) the cognition-driven decision process has implications for reducing information overload. Information is retrieved in the light of cases and the executive's SA and mental models. The retrieved information is the most closely connected with current decision situation.

Acknowledgement

This research is partially supported by Australian Research Council (ARC) under discovery grants DP0559213 and DP0557154.

References

[1] J. Q. Chen and S. M. Lee, *An exploratory cognitive DSS for strategic decision making*, Decision support systems, 36 (2003), pp. 147 -160.

[2] J. P. Shim, M. Warkentin, J. F. Courtney, D. J. Power, R. Sharda and C. Carlsson, *Past, present, and future of decision support technology*, Decision Support Systems, 33 (2002), pp. 111-126.

[3] D. Arnott and G. Pervan, *A critical analysis of decision support systems research*, Journal of Information Technology 20 (2005), pp. 67-87.

[4] F.-Y. Kuo, *Managerial intuition and the development of executive support systems*, Decision Support Systems, 24 (1998), pp. 89-103.

[5] M. R. Endsley, *Toward a theory of situation awareness in dynamic systems.*, Human Factors, v37(1) (1995), pp. 32-64.

[6] M. J. Adams, Y. J. Tenney and R. W. Pew, *Situation awareness and the cognitive management of complex systems*, Human Factors, 37 (1995), pp. 85-104.

[7] K. Smith and P. A. Hancock, *Situation awareness is adaptive, externally directed consciousness*, Human Factors, 37 (1995), pp. 137-148.

[8] C.-H. Chen and X. Ge, *The design of a web-based cognitive modeling system to support ill-structured problem solving*, British Journal of Educational Technology, 37 (2006), pp. 299 -302

[9] P. N. Johnson-Laird, V. Girotto and P. Legrenzi, *Mental models: a gentle guide for outsiders*, Sistemi Intelligenti, 9 (1998), pp. 68-33.

[10] R. Lipshitz, G. Klein, J. Orasanu and E. Salas, *Taking stock of naturalistic decision making*, Journal of Behavioral Decision Making, 14 (2001), pp. 331-352.

[11] S. K. Singh, H. J. Watson and R. T. Watson, *EIS support for the strategic management process* Decision Support Systems 33 (2002), pp. 71-85

[12] M. R. Endsley, B. Bolte and D. G. Jones, *Designing for situation awareness: an approach to user-centered design*, Taylor&Francis, London, 2003.

[13] EconomistIntelligenceUnit, *What do companies want from business intelligence?*, Economist Intelligence Unit, 2006.

[14] K. M. Sutcliffe and K. Weber, *The high cost of accurate knowledge*, Harvard Business Review, 81 (2003), pp. 74-82.

[15] R. Bergmann, *Experience management: Foundations, development methodology, and internet-based applications*, Springer-Verlag, Berlin, 2002.

[16] K. Carley and M. Palmquist, *Extracting, representing and analyzing mental models*, Social Forces, 70 (1992), pp. 601–636.

End-to-end Web Application Security

Úlfar Erlingsson Benjamin Livshits Yinglian Xie
Microsoft Research

Abstract

Web applications are important, ubiquitous distributed systems whose current security relies primarily on server-side mechanisms. This paper makes the end-to-end argument that the client and server must collaborate to achieve security goals, to eliminate common security exploits, and to secure the emerging class of rich, cross-domain Web applications referred to as Web 2.0.

In order to support end-to-end security, Web clients must be enhanced. We introduce *Mutation-Event Transforms*: an easy-to-use client-side mechanism that can enforce even fine-grained, application-specific security policies, and whose implementation requires only straightforward changes to existing Web browsers. We give numerous examples of attractive, new security policies that demonstrate the advantages of end-to-end Web application security and of our proposed mechanism.

1 Introduction

Web applications provide end users with client access to server functionality through a set of Web pages. These pages often contain script code to be executed dynamically within the client Web browser.

Most Web applications aim to enforce simple, intuitive security policies, such as, for Web-based email, disallowing any scripts in untrusted email messages. Even so, Web applications are currently subject to a plethora of successful attacks, such as cross-site scripting, cookie theft, session riding, browser hijacking, and the recent self-propagating worms in Web-based email and social networking sites [2, 17, 24]. Indeed, according to surveys, security issues in Web applications are the most commonly reported vulnerabilities on the Internet [16].

The problems of Web application security are only becoming worse with the recent trends towards richer, "Web 2.0" applications. These applications enable new avenues of attacks by making use of complex, asynchronous client-side scripts, and by combining services across Web application domains [8]. However, the shift towards Web 2.0 also presents an opportunity for enhanced security enforcement, since new mechanisms are again being added to popular Web browsers.

Therefore, we believe it is time to rethink the fundamentals of Web application security. It is our position that the client Web browsers must be given a greater role in enforcing application security policies. In this paper, we support our position with examples and a simple end-to-end argument: constraints on client behavior are enforced most reliably at the client. We also propose *Mutation-Event Transforms*: a novel, flexible mechanism for client-side security policy enforcement.

1.1 Motivating Attacks

Of the current attacks on Web applications, those based on *script injection* are by far the most prominent. For example, script injection is used in cross-site scripting [1] and Web application worms [2, 24].

A script injection vulnerability may be present whenever a Web application includes data of uncertain origin in its Web pages; a third-party comment on a blog page is an example of such untrusted data. In a typical attack, malicious data with surreptitiously embedded scripts is included in requests to a benign Web application server; later, the server may include that data, and those scripts, in Web pages it returns to unsuspecting users. Since Web browsers execute scripts on a page with Web application authority, these returned scripts can give attackers control over the users' Web application activities [1, 22].

Script injection attacks typically affect non-malicious users and succeed without compromising Web application servers or networks. For example, in 2005, the self-propagating Samy worm on MySpace used script injection to infect over a million users [24]. As a MySpace user viewed the MySpace page of another, infected user, the worm script would execute and send a page update request to the server, causing the worm script to be included also on the viewing user's page.

In an attempt to prevent script injection, most Web application servers try to carefully filter out scripts from untrusted data. Unfortunately, such data sanitization is highly error prone (see Section 2.1). For example, the Samy worm evaded filtering, in part, by the unexpected placement of a newline character [24].

Script injection is just one means of attack: there are many ways to exploit Web applications by presenting them with attacker-chosen data. As we demonstrate in this paper, end-to-end Web application security is not only a reliable means to prevent these attacks. Our proposals for enhanced, client-side security enforcement also form a simple, flexible foundation for the general security of Web applications, including future, more complex Web 2.0 applications.

2 The Case for End-to-end Defenses

In general, it is often best to establish systems guarantees at the point where they are needed, with an end-to-end check, rather than with earlier, piecemeal checks [21].

This end-to-end argument applies directly to Web application security. Although security policies should be determined and specified at the server, enforcement of policies about Web client behavior should be guaranteed at the client. The corresponding server-side checks are difficult to perform and, in practice, incomplete in ways that enable attacks.

2.1 Server-side Defenses and their Limitations

Web applications must consider the possibility of malicious attackers that craft arbitrary messages, and counter this threat through server-side mechanisms.

However, to date, Web application development has focused only on methodologies and tools for server-side security enforcement (for instance, see [11, 13]). At most, non-malicious Web clients have been assumed to enforce a rudimentary "same origin" security policy [22]. Web clients are not even informed of simple Web application invariants, such as "no scripts in the email message portion of a page", since clients are not trusted to enforce security policies.

This focus on centralized server-side security mechanisms is shortsighted: server-side enforcement has difficulties constraining even simple client behavior. For example, to enforce "no scripts", the server must correctly model complex, dynamic client activities such as string manipulation, and take into account all possible client features and bugs. This entails server consideration of a myriad different tags, encodings, and operators for comments and quoting [20].

Server-side removal of scripts is especially difficult for Web applications that wish to allow visual formatting or other data richer than simple text. As shown below, there are many non-obvious means of causing code execution, including within formatting tags:

```
<SCRIPT/chaff>code</S\0CRIPT>
<IMG SRC=" &#14;  code">
<STYLE>li {list-style-image: url("code");}</STYLE>
<DIV STYLE="background-image:\0075\0072\006C...">
```

Furthermore, server-side enforcement is unsuitable for Web 2.0 cross-domain mashups [25], which may access third-party servers to load code and data. For instance, Web clients perform such access whenever a Web application embeds the Google Search AJAX API [5].

2.2 Client-side Defenses and their Benefits

As described above, many security policies are best enforced at the client. Web clients are the final authority on client behavior—including where script code is found, what that code is, and from where the code was loaded. If informed of Web application security policies by the server, properly enhanced clients could reliably enforce those policies.

```
HTMLDocument.prototype.__defineGetter__(
    "cookie",
    function(){ return null; }
);
```

Figure 1: A programmatic security policy that will reliably disallow all script access to document cookies in many existing Web browsers, if included at the top of pages returned by a Web application server [3].

At the same time, the majority of users are not malicious, and would enable client-side enforcement to avoid exploits such as cross-site scripting and Web-based worms. Even if only benign users with enhanced clients might perform security enforcement, those users would be protected, and all users would benefit from fewer attacks on the Web application.

Unfortunately, there are many obstacles to the adoption of new, enhanced security mechanisms in popular Web browsers. Even when such enhancements are practical and easy to implement, they may not be deployed widely. Therefore, to increase its chance of widespread adoption, a Web client security mechanism should be practical, simple, and flexible, and be able to enforce multiple, attractive policies on client behavior.

3 New Client-side Security Mechanisms

In this paper we propose enhancing Web clients with new security mechanisms that can not only prevent existing attacks, but are able to enforce all security policies based on monitoring client behavior. In particular, our new mechanisms support policies that range from disallowing use of certain Web client features (e.g., IFRAMEs or OBJECTs) to fine-grained, application-specific invariants such as taint-based policies that regulate the flow of credit-card information input by the user.

Concretely, we propose that client-side enforcement proceed through a new client mechanism: *Mutation-Event Transforms*, or METs. METs are introduce here; some details like how to prevent their subversion are in Appendix A. METs allow Web application security policies to be specified at the server in a programmatic manner, such that those specifications can be used directly for enforcement at the client. In this, METs are similar to the code in Figure 1, and recent proposals such as BEEP [9].

In short, with METs, Web application servers specify security policies as JavaScript functions included at the top of pages returned by the server, and run before any other scripts. At runtime, and during initial loading, these MET functions are invoked by the client on each Web page modification to ensure the page always conforms to the security policy. Before a mutation takes effect, METs have the ability to transform that mutation, and the code and data of the page, which gives METs great flexibility in enforcement. In particular, METs can

be used to implement inlined reference monitors and edit automata for security-relevant client events, which allows METs to be used to specify and enforce any security policy based on monitoring client behavior [4, 26].

METs are both simple and straightforward to adopt: Web clients need only implement a single new primitive for mutation-event callbacks, and expose already-present events and data structures. Because policies are programmatic, they can readily account for browser variation and properly limit client-side enforcement on legacy Web clients (indeed, JavaScript code is already commonly used for compatibility and debugging purposes). Furthermore, security policy enforcement using METs requires only reasonable assumptions about the attacker.

3.1 Assumptions about the Attacker

METs can reliably defend against powerful attackers that are able to present Web clients with arbitrary code and data. In particular, the attacker may be modeled as an arbitrary, malicious script within Web application pages that are subject to MET enforcement.

The correctness of MET enforcement is of concern only to non-malicious users; it relies on network integrity and depends on assumptions about the server and clients. We trust that the Web application server has not been compromised, and properly includes METs at the top of returned Web pages; however, we assume that server code may have bugs such that the returned pages may contain arbitrary attacker-chosen data. We trust the Web clients to execute METs with proper semantics and to correctly enforce the fundamental same-origin policy [22]. Finally, we trust the programmatic security policies and that they correctly reflect the security goals of the Web application developers.

4 Policy Specification and Enforcement

Web application developers must have freedom in choosing security policies, and how they are derived. We propose specifying security policies using programmatic MET callback functions written in JavaScript. At runtime, these MET callback functions operate on each new (or updated) Web page and ensure that it conforms to the security policy, either through validation or transformation of the code or data within the Web page.

As we demonstrate in this section, METs have the appealing property that simple policies are easy to specify and enforce (much as in Figure 1). Even so, although Web application developers may guide security enforcement with Web page annotations, code for METs is likely to come as pre-packaged libraries, or be determined automatically at the server.

In particular, METs can be used for client-side enforcement of application-specific *dynamic security policies* determined automatically at the server from the natural constraints imposed by the structured composition of client pages (e.g., using frameworks such as ASP.NET AJAX [14] or GWT [6]). METs can also enforce other rich policies, such as those that apply to Web 2.0 cross-domain mashups [25], where application pages are composed outside the scope of server enforcement.

4.1 Examples of General, Basic Security Policies

On the following page, Figure 2 describes examples of general policies that apply to client Web pages, their script code, and the nodes and attributes of document data. On the same page, Figure 3 shows how these policies can be readily instantiated using MET callback functions; this code should be read in conjunction with Appendix A. In what follows, these policies are referred to by their number, in parentheses.

Policies (1), (3), and (6) are examples that restrict potentially dangerous types of document nodes, allow scripts only in certain portions of the document, or limit scripts to a whitelist of trusted scripts (as in [9]).

Policies (2), (4), and (5) validate the structure of certain data structures and scripts in Web pages, which can prevent many attacks (e.g., attacks that use malformed SQL queries [23]). Without such validation, malicious attacks may exploit may benign client-side code by presenting it with malformed data. For instance, without enforcement of policy (5), the Web client may at any time execute new, unexpected code where only a data return value was expected. (Client-side data validation may also reduce the number of round trips to the server.)

As shown in policies (7) through (9), the set of policies supported by METs are not restricted to actions that change the document structure of Web pages. METs can also support constraints on network access or access to security-critical client variables, such as the Web browser history, and enforce containment scopes between client-side gadgets and modules.

Finally, as demonstrated by (10), security policies based on METs may even include the code for a security-enhanced JavaScript interpreter, and ensure that it is used to execute all script code. Such a custom interpreter can implement dynamic taint propagation or other complex security policies.

For reasons of space, our example METs use several support routines, that would naturally be defined by security policy code. For example, the `matchURLDomain` function in (8) might match string URLs in a policy-specific manner, while the `outmostAttr` function in (9) might recursively walk up the document tree in order to find the attribute definition closest to the root. Similarly, policy-specific variables may encode security-relevant state such as in (1) for allowed ActiveX GUIDs (e.g., the Flash player), and in (2) the identity of a particular node in the document structure of a Web page.

(1) Disallow certain dangerous nodes or attributes. For instance, <IFRAME> nodes might be disallowed, and <OBJECT> nodes only permitted when instantiating the Flash player with known content.

(2) Data invariants on certain document subtrees. The Web page document is subject to invariants, even when modified dynamically at the client; e.g., blog comments must be a well-formed list of <DIV> nodes.

(3) Disallow scripts in certain parts of a Web page. A special case of (2), for instance to disallow use of <SCRIPT> nodes in untrusted blog comments.

(4) Scripts match valid, server-defined templates. An application of (2) to scripts: new, client-defined scripts may be allowed, but, for example, the onHover script code for a dynamically-inserted list item might be required to match `highlight(identifier)`.

(5) Cross-domain scripts return only data, properly. Instantiating (4) to prevent unexpected introduction of new code by cross-domain client-mashup applications: for instance, any script returned into a cross-domain <SCRIPT> node must have a syntax tree that matches `ajaxCallback(jsonDataValue)`.

(6) Limit scripts to a static, server-defined set. A static form of (4) that may simply match the hash of the script source text against a fixed "whitelist".

(7) Constrained access to object fields and methods. For instance, giving partial access to `document.cookie`, or limiting arguments to network-access methods.

(8) Proper network access via (cross-domain) URLs. URLs are subject to access control—both node-attribute URLs (e.g., on <IMG>) and the URLs used programmatically in scripts, (e.g., in an XML request).

(9) Containment of script activity to certain subtrees. Scripts can only modify certain document subtrees; thus, a gadget (or client-side mashup) for Web search might only be allowed to mutate a <DIV> for search results.

(10) Script execution by a secure interpreter. Scripts are not executed directly, but through a special, security-enhanced interpreter that may enforce (8), above, or even more fine-grained policies, such as variants of stack inspection or data tainting [4, 13].

Figure 2: A selection of attractive client-side security policies that can be readily enforced using programmatic MET callback functions. This list emphasizes general, widely applicable policies, while application-specific dynamic security policies are discussed further in the text (in particular in Section 4.2).

Type signature for MET callback functions

```
ExtendedNode
MET_callback(in Node script, // source of mutation
             in Node target, // target in Web page
             in ExtendedNode oldValue,
             in ExtendedNode newValue);
```

Example programmatic MET callback policies

(1) Limit OBJECT nodes (on OBJECT events):

```
var ok = (newValue.classid == theAllowedGUID);
return (ok) ? newValue : null;
```

(2) Data invariant on inserted DIVs (on DIV events):

```
if (target.id != insertionParentID) return null;
if (oldValue != null) return null;
var ok = ExtDOM.MatchStructure(newValue,
                "<div><ul><li></li></ul></div>");
return (ok) ? newValue : null;
```

(3) Limit script placement (on SCRIPT events):

```
var ok = ! findParentAttr("no_scripts", target);
return (ok) ? newValue : null;
```

(4) Restrict the code in scripts (on SCRIPT events):

```
var ok = ExtDOM.MatchScriptStructure(newValue,
                "highlight('identifier');"
return (ok) ? newValue : null;
```

(5) Proper data in AJAX replies (on SCRIPT events):

```
if (! newValue instanceof ScriptBody) return null;
var ok = ExtDOM.MatchScriptStructure(newValue,
                "callback({count: i; sum: 5;});"
return (ok) ? newValue : null;
```

(6) Script whitelisting (on SCRIPT events):

```
var ok = whitelist[ hash(newValue.toString()) ];
return (ok) ? newValue : null;
```

(7) Disallow history access (on SCRIPT events):

```
if (! newValue instanceof ScriptBody) return null;
return ExtDOM.ReplaceScriptLiteral(newValue,
            "history", "fresh_unused_literal");
```

(8) Limit network access (on SCRIPT events):

```
var ok = matchURLDomain(newValue.src, "foo.com");
return (ok) ? newValue : null;
```

(9) Script containment (on any mutation event):

```
var src = outmostAttr("containment", script);
var dst = outmostAttr("containment", target);
return (src == dst) ? newValue : null;
```

(10) Secure interpreter (on SCRIPT events):

```
if (! newValue instanceof ScriptBody) return null;
var arg = ExtDOM.CreateScriptNode("Arguments",
                newValue.ToJSON());
var func = "special_js_interpreter";
return ExtDOM.CreateScriptNode("Call", func, arg);
```

Figure 3: The type signature of MET callback functions and several possible implementations for policies like those in Figure 2. The details in Appendix A are relevant to this code. Due to space constraints, only terse, uncommented code is shown and the functionality of policy-provided variables and methods is indicated by name.

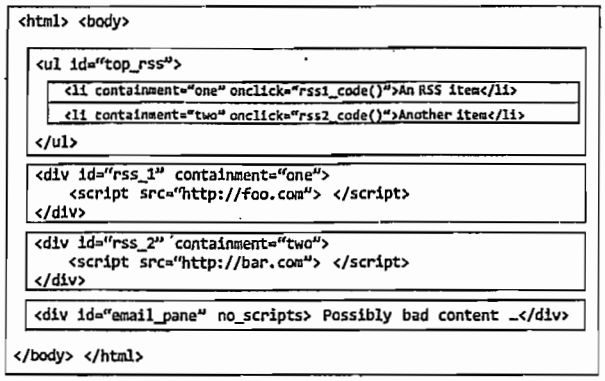

Figure 4: An outline of the document tree for an aggregation Web page that contains both RSS news items and email messages.

4.2 Application-Specific, Dynamic Security Policies

Policies can also be highly application-specific. Such policies can be either hand-written by the application developer or generated through static analysis of the Web application. This is illustrated by the examples below.

Example 1. Access control within a page. Figure 4 shows an example of a DOM tree containing data from two RSS sources: `rss_1` and `rss_2`. We would like to make sure that `rss2_code` does not modify the first `<div>` element so that it is impossible to have a rogue RSS feed that changes the contents of another one. Using policy (9), we can restrict code to modify only DOM elements declared within the same scope. This policy allows isolation of code and data on a single page, and refines the "same-origin" policy of existing Web clients.

Figure 4 also shows how security policy can be directed by inline attributes on document nodes. In this case, a `no_scripts` attribute is used to direct MET enforcement of a policy such as (3) in Section 4.1.

Example 2. Google Web Toolkit (GWT). In GWT, the developer writes his or her application in Java [6]; the application is subsequently compiled by the GWT into two parts: a Java part that resides on the server and a JavaScript part that resides on the client. Unfortunately, given a client-side attack, the assumptions of the original Java application may not hold for the scripts at the client,

To prevent this, the server may generate policies that enforce consistency properties of the client code. For example, the server may wish to ensure that access control properties such as "a private method may only be invoked by methods in the same Java class" present in the original Java source code are preserved in the JavaScript code on the client side. Instantiation of such a policy would be application-dependent and could be obtained through static analysis of the original Java code.

Example 3. Server-generated content templates. Dynamic policy generation is also relevant to ASP.NET or JSP pages. Both of these technologies allow servers to mix static HTML and dynamic content. Using static analysis (e.g., that in [15]), the computed parts of Web pages can be approximated and, thereby, the structure and contents of generated pages. For example, the analysis may be directed to assume no permitted scripts in application inputs. Such page "templates" are highly suitable for client-side enforcement.

5 Discussion

End-to-end Web application security entails preventing client behavior and server interaction that should be impossible, by construction, or has otherwise been determined to be illegal. Whether policies are driven by automatic analysis, or by manual setting of policy, there is much to gain from this form of security. In particular, it is a necessary foundation for securing Web 2.0 applications like cross-domain mashups, which are often outside the scope of existing mechanisms.

Mutation-event transforms, or METs, are an attractive option for client-side security. METs are flexible enough to enforce any security policy based on execution monitoring [4, 26]. In particular, METs readily allow precise enforcement of policies on both code and data (e.g., such as those in [23]). At the same time, METs, and their supporting code, should be straightforward to implement, since they rely only on existing browser events and data structures.

In comparison, the servers can leverage the "same origin" security policy [22] to enforce some client-side policies, as done in SessionSafe [10]. Such schemes require multiple, elaborate server domains that may be cumbersome to manage. Even so, they can provide only limited, coarse protection such as disallowing access to Web application cookies—as in policy (7) in Section 4.1.

Some previous proposals enforce client-side security policies by making use of separate proxies to rewrite server requests from the Web client. Noxes [12] places simple restrictions on the URLs of requests. BrowserShield [19] and CoreScript [26] use elaborate script rewriting techniques to enforce policies such as disallowing cookie access and dangerous tags—as in policies (1) and (7) in Section 4.1. Although they are useful (e.g., for legacy support), such proxy-based mechanisms must correctly parse data and code in requests, which can be a near-intractable problem, even using structured, formal methods (see Section 2.1 and [26, Section 6]).

Indeed, like METs, reliable mechanisms for client-side security policies must necessarily build on the final parsing of code and data performed at the Web client. This approach has been taken in previous mechanisms, most notably in BEEP [9], but also in [7]. However, these proposed mechanisms have provided little flexibility in security policy specification and enforcement, only supporting policies like (3), (6), and (7) in Section 4.1.

The enforcement of end-to-end security policies offers benefits to all Web application users, but requires changes to existing Web browsers. The inclusion of our proposed METs mechanisms in Web clients can reliably prevent existing attacks and provide a flexible, fine-grained foundation for the enforcement of future application-specific security policies

References

[1] CGI Security. The cross-site scripting FAQ. http://www.cgisecurity.net/articles/xss-faq.shtml.

[2] E. Chien. Malicious Yahooligans. http://www.symantec.com/avcenter/reference/malicious.yahooligans.pdf, 2006.

[3] S. Di Paola. Wisec security. http://www.wisec.it/sectou.php?id=44c7949f6de03, 2006.

[4] Ú. Erlingsson and F. B. Schneider. IRM enforcement of Java stack inspection. In *Proc. IEEE Security and Privacy*, 2000.

[5] Google AJAX search API. http://code.google.com/apis/ajaxsearch.

[6] Google Web toolkit. http://code.google.com/webtoolkit.

[7] O. Hallaraker and G. Vigna. Detecting malicious JavaScript code in Mozilla. In *Proc. IEEE Conf. on Engineering of Complex Computer Systems*, 2005.

[8] B. Hoffman. Ajax security. http://www.spidynamics.com/assets/documents/AJAXdangers.pdf, 2006.

[9] T. Jim, N. Swamy, and M. Hicks. Defeating script injection attacks with browser-enforced embedded policies. In *WWW*, 2007.

[10] M. Johns. SessionSafe: Implementing XSS immune session handling. In *Proc. ESORICS*, 2006.

[11] N. Jovanovic, C. Kruegel, and E. Kirda. Pixy: A static analysis tool for detecting Web application vulnerabilities. In *Proc. IEEE Symp. on Security and Privacy*, 2006.

[12] E. Kirda, C. Kruegel, G. Vigna, and N. Jovanovic. Noxes: A client-side solution for mitigating cross-site scripting attacks. In *ACM Symp. on Applied Computing*, 2006.

[13] B. Livshits and M. S. Lam. Finding security errors in Java programs with static analysis. In *Proc. Usenix Security Symp.*, 2005.

[14] Microsoft ASP.NET AJAX. http://ajax.asp.net.

[15] Y. Minamide. Static approximation of dynamically generated Web pages. In *Proc. WWW*, 2005.

[16] MITRE. Common vulnerabilities and exposures. http://cve.mitre.org/cve/, 2007.

[17] Open Web Application Security Project. The ten most critical Web application security vulnerabilities. http://umn.dl.sourceforge.net/sourceforge/owasp/OWASPTopTen2004.pdf, 2004.

[18] T. Pixley. DOM level 2 events specification. http://www.w3.org/TR/DOM-Level-2-Events, 2000.

[19] C. Reis, J. Dunagan, H. Wang, O. Dubrovsky, and S. Esmeir. BrowserShield: Vulnerability-driven filtering of dynamic HTML. In *Proc. OSDI*, 2006.

[20] RSnake. XSS (Cross Site Scripting) cheat sheet. http://ha.ckers.org/xss.html, 2006.

[21] J. H. Saltzer, D. P. Reed, and D. D. Clark. End-to-end arguments in system design. *ACM Transactions on Computer Systems*, 2(4):277–288, Nov. 1984.

[22] Same origin policy. http://en.wikipedia.org/wiki/Same_origin_policy, 2007.

[23] Z. Su and G. Wassermann. The essence of command injection attacks in Web applications. In *Proc. POPL*, 2006.

[24] The Samy worm. http://namb.la/popular.

[25] Web Mashup. http://www.webmashup.com.

[26] D. Yu, A. Chander, N. Islam, and I. Serikov. JavaScript instrumentation for browser security. In *POPL*, 2007.

A Mutation-Event Transforms

Here, we present some details on METs, our proposed new mechanism for flexible client-side enforcement.

Mutation events are defined in the proposed Document Object Model (or *DOM*), level-2, as events caused by any action that modifies the document structure [18]. METs are similar to, but simpler than, these standards proposals. METs are also more expressive since they operate on extended data that include both the standard DOM tree model [18] and the abstract syntax trees (ASTs) of executable scripts. Both mutation events and the ASTs of scripts are abstractions already implemented in Web clients; thus, support for the METs primitive should not require substantial client additions or changes.

Importantly, METs provide two mutation events for <SCRIPT> nodes: first, an event when the script node is inserted in the DOM, and another event when that inserted node is populated with the AST for its script code. This separation allows METs to enforce security policies that limit network access caused by SRC host URL attributes in script nodes. Other nodes, such as <STYLE>, are also handled in this manner.

The type signature of MET callback functions is given at the start of Figure 3. Both the `script` and `target` are regular DOM nodes in the document tree. The `script` refers to the node containing the script that is attempting the document mutation (e.g., by writing to an `innerHTML` field). The `target` refers to the parent node where `newValue` is about to be inserted to replace `oldValue`. Both `oldValue` and the `newValue` are well-formed, properly nested subtrees of our extended DOM that includes ASTs; either may be `null` to denote empty subtrees. The callback functions return an extended DOM subtree to be used (instead of `newValue`).

MET callback functions may be registered for DOM elements of particular types, e.g., as follows :

```
add_MET_callback(nodeType, policy)
```

In the above, `policy` would be invoked whenever a DOM element of type `nodeType` is affected (i.e. inserted, replaced, or deleted). This would happen at runtime, right before the mutation, but after the Web client has parsed the new, proposed extended DOM values.

All programmatic security policy variables and functions, and MET callback registration, may naturally occur in the first <SCRIPT> tag of Web pages. To prevent subversion of security enforcement, the script language scoping rules (or other means) should prevent access to security policy code and further MET callback registration might be disabled, e.g., by simply setting `document.prototype.add_MET_callback` to `null` in the code. More flexibly, Web clients might allow other scripts to register MET callback functions, if they carefully ensure security policy always takes precedence.