2008

Mediated Internet Experience for Senior Citizens

Rajarshi Chakraborty
University of Buffalo, rc53@cse.buffalo.edu

Raghav Rao
University of Buffalo, mgmtrao@buffalo.edu

Vidyaraman Sankaranarayanan
University of Buffalo, vs28@cse.buffalo.edu

Shambhu Upadhyaya
University of Buffalo, shambhu@cse.Buffalo.EDU

Mediated Internet Experience for Senior Citizens

Rajarshi Chakraborty
Computer Science and Engineering,
University at Buffalo
rc53@cse.buffalo.edu
Vidyaraman Sankaranarayanan
Computer Science and Engineering,
University at Buffalo
vs28@cse.buffalo.edu

Raghav Rao
School of Management,
University at Buffalo
mgmtrao@buffalo.edu
Shambhu Upadhyaya
Computer Science and Engineering,
University at Buffalo
shambhu@cse.buffalo.edu

ABSTRACT

Survey results from the Pew Internet American Life Project indicate that the demography of senior citizens that conduct activities on the Internet is rapidly growing and vulnerable to online privacy violations. Their enhanced vulnerability stems from their trusting nature, a characteristic of their times and culture. Since the Internet related threats such as phishing, spamming, etc., are still research issues, a purely technical solution, although desirable, is currently not viable. In this paper, we view the problem through the trust prism and argue for a socio-technical solution to help senior citizens conduct their online activities safely. We propose the conceptual outlines of a trust based framework for a Mediated Internet Experience (MINE) for senior citizens residing in a community center. The framework uses a trust model based on Bayesian Network modeling to help assign trust levels to Internet sites and recommend them for further transactions. Towards a realistic expansion and implementation of the proposed framework and trust model, we propose to conduct surveys and statistical analysis.

Keywords

Privacy, senior citizens, Bayesian Network, recommender systems, conceptual framework.

1. INTRODUCTION

Senior citizens are the fastest growing demographic group of online users, yet are also amongst the most vulnerable. Information and communication technologies (ICTs) are an important communication source enabling older people to combat social isolation through access to information and social activities [11]. However, there are growing concerns with regard to information privacy and the risks of the ageing population in this regard in the UK and Europe.

The threats faced by senior citizens on the Internet are prominent and can be attributed to two main reasons. First, they grew up in a more honest world and tend to be trusting of other people. Secondly, most seniors do not spend as much time on the Internet as younger consumers ("grey digital divide") and are not as knowledgeable about Internet frauds. One of the biggest factors that affect senior citizens both positively and negatively when using the Internet is that the concept of trust among this demography is very different from that of the rest of the population. This claim can be backed up by the results of numerous surveys conducted in the past.

In this work, we first examine the threat vectors related to Internet Browsing that seniors are most vulnerable to. Given the fact that most of these threats (like phishing, spam, etc.) are topics of active research, it is apparent that there is no single solution that can be proposed to 'solve' the problem *per se*. Instead, we argue that the problem is more a manifestation of trust expressed by the senior citizens in their environment, and thus requires a trust based approach to address the problems. Viewing the problem from a 'trust' prism, we propose a trust based network model to provide an enhanced and mediated Internet experience for senior citizens within the confines of the community homes. This trust model is based on a game theoretic framework where the senior citizens are modeled as players; their browsing actions constitute their strategies in the model. We show how the trust model evaluates the trustworthiness of each user based on their browsing patterns. Based on the evaluated trustworthiness, we provide an enhanced browsing experience where senior citizens are given appropriate cues based on the current context and their trust level.

Thus, the contributions of this paper may be summarized as follows:

- We investigate the major threat vectors that senior citizens are most vulnerable to and argue for the need to view the issue through the prism of trust
- We present BANETS, a Bayesian Network based trust model to dynamically evaluate the trust factor for each Internet user (senior citizen) based on the current context and browsing history
- We design the "Mediated Internet Experience" (MINE) framework that uses the BANETS trust model to provide context specific cues for senior citizens during a typical browsing experience

The contributions of this paper also set up a platform to address research issues such as how to mathematically model the numerous human factors primarily responsible for defining the behavior of the senior citizens.

The rest of the paper is organized as follows. Section 2 presents related work. Section 3 presents the Threat vectors that Senior Citizens are most vulnerable to and argues for a trust based socio-technical solution approach. Section 4 presents the Bayesian Network graph based Trust Model (BANETS), which is subsequently used by the MINE framework in section 5. Section 6 presents concluding remarks and lays the ground for future work.

2. RELATED WORK

A literature survey reveals that there has been sufficient work in online privacy protection for the population in general but there has not been any research geared specifically towards the senior citizens. We believe our research is the first attempt to investigate the online privacy issues of senior citizens. The difference between the senior citizen demography and the contemporary Internet savvy generation presents the need to look into systems that enhance trust for websites and online services by building reputation for them as well as the activities of the users themselves.

Recent work on reputation-based trust frameworks and collaborative filtering systems show that its application is extremely widespread. They have already been implemented as part of successful commercial systems [6]. Distributed systems do not help where a big subset of the users for whom trust is required, trust building is conducted passively from a central entity.

Most of the commercial systems surveyed above have a centralized architecture, where the reputation about one participant is collected by other participants. Such a framework though appealing doesn't suit the problem of mediated Internet experience. For the problem addressed by this paper, reputation of each participant is not required – what is required is the reputation about certain online activities based on the experience of these users. The experiences vary based on certain parameters (age, prior education) of the users. This presents a layered structure of the problem at hand. A broker framework for web applications [8] comes very close to addressing our problem but falls short by assuming that each participant has to carry the burden of sharing feedback. This task assignment cannot be expected from certain subcategories of senior citizens who need more than average amount of handholding on the Internet. A considerable amount of work has been done on reputation systems for peer-to-peer networks [10, 14] and sensor networks [5]. Recommender systems based on reputation have been used in skiing to help enthusiasts learn about routes, weather conditions, etc [2]. A crucial factor missing in these actions are the intervention both before and runtime for the participants when a fault occurs despite a low or bad reputation. The BANETS model and the MINE framework presented in this paper principally differs from previous works in that aspect. i.e., mediated browsing experiences to help senior citizens fully utilize the Internet for their needs.

3. THREAT VECTORS

In the Unites States, according to the Pew Internet American Life Project (2004), 22% of Americans 65 and older used the Internet in 2004, which went up from 15% in 2000. In 2006, 34% of Americans age 65 and older went online [4]. "Wired" seniors use the Internet in order to do various activities: 66% looked for health or medical information in the online; 66% conducted the product research on the Internet; 60% visited Government websites; 47% have done online shopping; 41% used the Internet to make travel reservations; and 20% are using Internet banking, These statistics reflect the lifestyle of an average senior citizen. This makes it imperative to understand the threats associated with such online activities. Most senior citizens suffer from health problems and they engage in research about symptoms, remedies and cure of these problems. The Internet is naturally one of the best resources of such information. This can be easily taken advantage of by some malicious party. A phishing website can take advantage of this curiosity of the senior citizens by promising relevant health information by asking personal information. Spammers on the other hand, especially those with an agenda of stealing private information, can send out information about bogus products that look extremely close to the information sought by the senior citizens. If the senior citizen is enticed enough to look further, he or she might land up in a potential trap to share personal / private information.

The low usage of Internet Banking among senior citizens compared to the other activities, especially online shopping is almost obvious since banking can sometimes involve many complications regarding accounts, depositing, withdrawing, loans, etc. The senior citizens perhaps feel more comfortable in conducting these activities face to face with bank personnel rather than trust a machine interface to answer all questions. This finding may also imply that there is room for improvement on making banking websites more user-friendly and convincing enough to a crowd of senior citizens that it will get the job done. *However, the lack of interest in online banking does not necessarily reflect the fear or perception of risk of having one's privacy intruded for the senior citizens.* This can prove to be an extremely vulnerable zone for attack since phishing emails from bank accounts is not uncommon. Phishing can also be a highly potential threat when visiting government websites and shopping online. Senior citizens have a special interest in Government related websites since they have concerns about legislations, information about social security and Medicare, pensions, loans and national security, and thus are extremely likely to fall prey to phishing emails from so-called government sites [13]. Online shopping is extremely convenient for most senior citizens since mobility becomes an issue for this demography especially in driving.

There is, however, a big caveat to the phenomenon of increasing use of the Internet by the senior citizens. They are extremely vulnerable to privacy attacks. According the testimony of David Jevans (the chairman of the Anti-Phishing Working Group) at the U.S. Senate Special Committee on Aging [1], the senior population makes appealing targets, and should be particularly careful of phishing attacks, because they potentially have the most to lose. Spamming about products catering to senior citizens poses another threat. This is true especially with medicines and other health-related products that many senior citizens would be more comfortable purchasing with more privacy and confidentiality.

Thus, the threat vectors for senior citizens may be summarized as follows:

- Internet Identity theft by means of phishing schemes (online banking)
- Fraudulent product recommendations for health related products and incorrect purchasing venues (online pharmacies)

Solution Approach

While these are the summary statements for the threat vectors, it is evident that the underlying thread is a violation of the trust senior citizens place on their Internet related experience. Thus, we argue that the problem may effectively be approached by a socio-technical approach rather than purely system oriented approaches such as anti-phishing toolbars, spam filters, etc. We intend to use these existing tools in our domain to provide us an indication of a problem (that can be used to forewarn our users - senior citizens). Thus, we have cast the problem in a more *user centric* manner, rather than relying solely on system specific approaches.

The ultimate goal of this research endeavor is to have a real-world deployment of our trust-based framework not just as some standalone application for the system administrator. The runtime trust evaluation and the framework have to be implemented as a distributed feedback-based software and hardware infrastructure. Given the dual need for privacy as well as customized protection of the subjects it is not too hard to foresee the need to have some of the feedback generating processes on the client systems work in a subtle if not stealth manner. This feedback information collected will validate and adjust the Bayesian Network based Trust model while the framework that takes decision or is told to take decision will be more centralized. The details of such a practical translation of our theoretical proposal are beyond the scope of this paper but definitely an essential next step.

An important post-hypothesis step for a feasible framework would be to take the help of the two relevant threat vectors discussed earlier. We wish to first implement a threat model using the Microsoft Threat Modeling Tool. This model will incorporate the information flow outlets and inlets, different scenarios of a senior citizen using the Internet and how these when combined enable the Phishing and Product Scam threat vectors. The population of these vectors at the initial stage will be done from separate pre-research surveys. These vectors will contribute actual values to the symbolic thresholds used for decision making by our system as described later. The method of generating these initial and/or standard values is beyond the scope of this paper as well.

A big advantage that we might have towards developing our solution methodology is that we are hoping that senior citizens are more likely to respond to system related messages such as dialog boxes, etc., that the regular user is now accustomed to ignoring, i.e., we may expect senior citizens to pay sufficient attention to system warnings and follow the appropriate cues rather than dismissing them. This would be easy to foresee because the generation of senior citizens on average show more patience than the contemporary generation. Besides the patience factor any generation is likely to pay more attention to tools and amenities that they have never been introduced before for a long time. With this background, we now present the trust framework that evaluates the trustworthiness of users and provides appropriate cues for a trustworthy browsing experience.

4. BANETS: BAYESIAN-NETWORK-BASED TRUST FOR SENIOR CITIZENS

Motivation for Selecting Bayesian Networks

Any system admin tool for attack protection can be designed in the most trivial fashion. In other words, it could be directed to monitor all its objects of protection and implementing rules that are as rigid as possible. But such systems have been designed long back and they lack novelty. The challenge lies in developing a framework that is “smarter” and almost emulates how a human system admin would process the information and react. This is where recommender systems come into play. The tool needs to act in a more nuanced way based on the recommendation/feedback it gets from its subjects about vulnerabilities or a lack thereof.

The basis for our recommender system is a Bayesian network model. This model allows us to represent how a set of actions can “influence” another by representing them as nodes in a weighted directed graph. The edge represents the direction of this influence and the weight reflects the conditional probability about the events. This helps in finding the joint probability of more than two actions which is compared them to pre-defined threshold values. These joint probabilities represent the various possible scenarios which can lead to a single outcome. A Bayesian model thus seems the most appropriate for the representation of the inter-dependence of actions by different parties in a system involving human beings where scenarios are plenty.

As presented in [15], conditional probability is a very natural choice of mathematical representation of the influence of an action of one kind (say A) on the occurrence of an action of another kind (say B). The uncertainty associated with either of these actions has to be represented in terms of probability. The probability of the success of an A action being conditional on the probability of the success of a B action in the past is reflective of numerous real world problems. It should be noted though that calculations for conditional probabilities based on the sum and product rules can become NP-hard even in the case of moderate number of random variables. Bayesian networks help in determining causal relationships. They are advantageous in the way independence of variables prevents the need to compute all the joint probabilities thus shortening the computation from exponential order to linear [15].

Bayesian Network for a non-monitored Senior Citizen

In this section we present the conceptual outlines of the Bayesian Network (BN) based trust model used for the recommender system that will help the System Admin tool for protecting the senior citizens. The recommender system will provide feedback and recommendation values of different online activities the residents of the community center engage in while on the Internet. It should be noted that one BN model is not enough to capture all the possible activities. On the other hand, presenting all the possible BN graphs to cover every possible Internet activity is beyond a feasible length of this paper. We thus present only one example of such a graphical model.

The trust model presented here captures a much generalized online pitfall as far as privacy is concerned. The aim is to find out if a website to be visited or already visited is good or bad. Most importantly this captures both fishing and spamming – the two of our prime privacy concerns with senior citizens. We also narrow down the scope further by providing the model for the youngest group of the senior citizens – age 65 to 70. We consider them to the most Internet savvy as intuitively people of generations any older than that were in their prime when computers and Internet weren’t. This has convinced us to break up the residents of the Community center into two major groups based on age. We do believe more survey results are required to establish this concretely.

We begin our discussion by presenting the different “nodes” in the Bayesian Network graph. Each of these represents an *action category* either by a human or by the System Admin. The cause and effect relationship between these two entities in the graph does not dictate how the System Admin should actually work. On the contrary their values are used against pre-defined thresholds for the Admin to work according to what comprises the other half of our proposed framework outline. The threshold values for the purpose of this paper are left as mathematical symbols but they need to be established by survey and statistical analysis to render our proposal more meaningful and plausible.

The cause and effect relationship is not restricted to human and machine. We completely recognize that when many people of the older generation share a common residence – in our case a Community Center - they are bound to interact much more frequently than an average person does with his/her neighbor or colleague. It is thus impossible to ignore the factor of influence of one user’s behavior on another, especially through word of mouth. For example, if senior citizen A bought groceries online from a certain website and A and another senior citizen B socialize enough, then it is very likely that the B will get a feedback about the website from A. This feedback could be positive or negative, where the positive will possibly influence B to more likely to visit that same website in future than how much the negative will. We are of course, for the sake of simplicity, discounting any pre-established trust between the users – rather we assume that trust about Internet usage grows with the passing of these feedbacks. To quantify these elements of trust, we need more statistical results. This human interaction has some parallels with the sociological patterns in dorms for college students, except that young students are more Internet savvy than our target demography and so any kind of remedy requires less central authoritarian intervention.

The Bayesian Network graph acts as a guideline for helping the System Admin "deal" with the actions and consequences of an individual senior citizen (aged 65-70) on the Internet. We label him/her as SeniorCitizenUser. As discussed above, we consider another person labeled FellowSeniorCitizenUser whose actions directly or indirectly influence SeniorCitizenUser. In future we aim to modify the graphs to incorporate not just a single human influence or for that matter single group (age group) influence, but multiple groups as well. This will help shorten the computation among other benefits.

Along with the title for each node of the above graph, in Table 1 we present the possible textual values that can result from the actions represented by that node. In plain English this means more than one actions (or none) could belong to a certain category. All the values for an action category come with a simple enumeration to help shorten the probability expressions presented later in this paper. Any value that begins with the word True or False means they are true or false in the universal sense for the senior citizen, respectively. e.g. FalseGood refers to a false perception that a website is good (i.e. not a phishing or spam site). Also each node title and its values are followed by an explanation about the activity category the node represents.

SiteReputation	Good (0), Bad (1), FalseGood (2), FalseBad (3)
	The reputation of the site for the users
SiteBlock	Yes (1), No (0)
	Whether the gateway of the System Admin blocks the site
SeniorCitizenUserBrowsing:	Visits website (1), Does not visit (0)
	The possibility of a SeniorCitizenUser visiting a website by following a link or typing an address
FellowSeniorCitizenUserBrowsing:	Visits website (1), Does not visit (0)
	The possibility of a FellowSeniorCitizenUser visiting a website by following a link or typing an address
SeniorCitizenUserBrowsingExperience:	FalseVictim (0), TrueVictim (1), FalseNonVictim (2), TrueNonVictim (3)
	The perception of the user after visiting a website; "NonVictim" indicates if the user does not feel threatened or unsafe
FellowSeniorCitizenUserBrowsingExperience	FalseVictim (0), TrueVictim (1), FalseNonVictim (2), TrueNonVictim (3)
	The perception of the user after visiting a website; "NonVictim" indicates if the user does not feel threatened or unsafe
Education	0, 1,..., n
	Education and training about Internet Usage can be divided into 'n' levels with 0-level being the most advanced and 'n' being most preliminary. Re-education means the earlier level didn't work and so the new workshop has to be simplified more.
Intervention	Yes (1), No(1).
	Intervention is needed when a user makes a mistake for a certain number of times or even once if he/she is extremely old. There could be a combination of factors that lead to an intervention – a few examples will be presented in the algorithmic description of the framework.

UpdtSiteTrustRepository	DontUpdate (0), UpdateSiteAsBad (1), UpdateSiteAsGood(2)
	The System Admin refers to a repository where trust values of the site being accessed are stored and updated based on feedback from the users and monitoring where the latter is needed for the higher age groups.

Table 1: Node titles and their values for the Bayesian Network Graph

Next we present the diagram (Figure 1) of Bayesian Network Graph representing how the different action categories influence each other. The direction of the influence is indicated by the direction of the edges in that graph. For example, the browsing experience of SeniorCitizenUser if universally real can influence updating the site's trust in the Repository. On the other hand, FellowSeniorCitizenUser's browsing experience, if bad, may lead to a bad reputation of the site. The intervention is only considered for the SeniorCitizenUser which influences the level of education or workshop. The experience of another user (FellowSeniorCitizenUser) only matters when it comes to direct contact or through site trust update. The reason we let both the Browsing action and after-Browse-Experience of FellowSeniorCitizenUser influence the Browsing action of SeniorCitizenUser is because FellowSeniorCitizenUser's avoidance of the site (due to knowledge gathered) can influence SeniorCitizenUser's decision as can FellowSeniorCitizenUser's experience, both through "word of mouth". This graph captures the simplest privacy scare and presents an enormous amount of possible scenarios that may or may not help, prevent or encourage materializing such a scare. Due to this enormity we present a very simplified and trimmed out version of what the framework for the System Admin will look like, in the next section.

5. MINE: MEDIATED INTERNET EXPERIENCE FRAMEWORK

The conceptual framework for mediated Internet experience for senior citizens (MINE) presented in this paper is simplified due to the overwhelming number of combinations of factors that can affect the actions and consequences inside an information system that has a potentially vulnerable demography like senior citizens as participants. The framework is based on the Bayesian Network graph in Figure 1 and its macro view is presented in Figure 2. MINE is described below in an algorithmic fashion. It is essential though to list out some of the key expressions used in this algorithm, some of which are joint probabilities based on the Bayesian Network graph presented already.

In Table 2, we present the concept of recommendation. Rec^+ is a true recommendation (not to be confused with positive recommendation), while Rec^- is a negative or false recommendation. A true recommendation can be either positive or negative. It is because of this open-ended nature of the parameter that we have chosen to use only a few example mappings between joint probability expressions and the recommendation terms. We define recommendation from the BN model as a probability of about the reputation of the site and the actions taken and the experience perceived by the SeniorCitizenUser and sometimes coupled with FellowSeniorCitizenUser's actions and their mutual interaction/feedback.

Rec$^+$	True Recommendation
Rec$^-$	False Recommendation
T_e	Threshold for lack of education / training required
$T_{BadSite}$	Threshold for Bad Sites
T_{RecPos}	Threshold for Positive Recommendation
T_{RecNeg}	Threshold for Negative Recommendation
T_{RecF}	Threshold for False Recommendation

Table 2: Expressions used for a MINE algorithm

The following are examples of mappings to Rec^+:

Rec$^+$	P(SiteReputation=0, SeniorCitizenUserBrowsing=1, SeniorCitizenUserBrowsingExperience=3)
Rec$^+$	P(SiteReputation=1, SeniorCitizenUserBrowsing=0,

	FellowSeniorCitizenUserBrowsingExperience=1)

Table3: Multiple mappings to framework variables

Table 3 gives a couple of examples of multiple mappings to a recommendation term. Here the first row says that if the reputation of the site is perceived to be good and the SeniorCitizenUser had a truly good experience, then it is a *true positive* recommendation / feedback about the site. On the other hand, in the second row, a bad reputation along with an established bad experience for the SeniorCitizenUser's friend, FellowSeniorCitizenUser, coupled with SeniorCitizenUser's avoidance show that it is a *true negative* recommendation about the site.

The next step towards realizing the conceptual framework is to list out the goals of the System Admin, especially in this paper for the youngest (65-70) and the most Internet savvy senior citizens. We have assumed that they don't need hand-holding and thus the System Admin should avoid monitoring their activities unless intervention is required. As Figure 2 shows, MINE must primarily act as a gateway, occasionally being alerted by mistakes or missteps or failures inside the network. We assume these alerting services to be in existence. These mechanisms could be incorporated into the BN graph thus rendering it even larger and more complicated. One interesting aspect of this design is that the thresholds are not simply functions of number of attempts. They rather take into account the number of attempts but still keep comparing with the threshold values which are to be obtained through surveys in future. The BN graph could suggest the MINE system to re-educate the senior citizen even if the site's reputation may not be changed in the repository. The following is a simplified workflow of the MINE with respect SeniorCitizenUser from the BN diagram.

```
1.  Educate User at level(i)
2.  Do not Monitor User
3.  If (Misstep detected / Attack reported)
    {   //pre-built alert to detect "stepping" into a bad site
        then
        if(max[P(Education=i,SeniorCitizenUserBrowsingExperience=1,
                FellowSeniorCitizenUserBrowsingExperience1),

    P(Education=i,SiteReputation=1,SeniorCitizenUserBrowsing=1,FellowSeniorCitizenUserBrowsing=0),
                      P(Education=i,FellowSeniorCitizenUserBrowsing=1,SeniorCitizenUserBrowsing=1)]
                              $< T_e$
                then
                Educate User at level(i+1)//Simpler education this time
         if($(Rec^+)^n > T_{BadSite}$)
                then
                System Admin must:
                1.  Update Site Trust to 0 in Repository
                2.  Block Site for SeniorCitizenUser              //The idea of blocking it universally will be
                    explored
                                                  //in the future
    }
4.  Get constant feedback / recommendations:
        1.  $(Rec^+)^n$ and $(Rec^-)^m$, n true recommendations and m false recommendations
        2.  Update Site Trust Repository only if
                $((Rec^+(SiteReputation=0))^n > T_{RecPos}$
```

The workflow presented above is a small sample of the amount of work the System Admin needs to be doing for the most Internet savvy senior citizens in the community center. The framework will most likely be in the similar spirit as the Lumiere project was used for the Microsoft Office Clippy [17]. The MINE framework's structural outline is similar to [7], where the authors proposed a reputation based trust framework for web applications. The other work that is most similar to this concept is the Moleskin [3] framework which is also based on recommendations. MINE differs from these works in that the core trust model used is BANETS, which is tuned for the senior citizens domain, instead of customizing generic recommendation systems that rely on users knowledge.

The MINE framework would be deployed in three distinct stages. In the first stage, detailed surveys would be carried out to classify and understand the target demographic. The comfort level of senior citizens with respect to computer usage, adaptability, etc., will be gauged. The categorization of the senior citizens for the forming the BN graphs can be obtained from such surveys. The second stage is an education phase, where multimodal means of communicating the threats of the Internet to the user base (like the phil game [12]) will be considered. Once the second phase is complete, the third phase, which involves the deployment of a client on all systems in the community center, will be initiated. This client shall be responsible for implementing the BANETS model. This involves system specific issues like becoming an add-in to the browser, monitoring the browsing history, detecting phishing sites and evaluating the trust values of every site. The actual computation, however, shall be performed on a centralized server that is present in the community center. Finally, the BANETS model requires certain probability values that would help make the model more concrete. The parameters that these functions depend on will be derived from the surveys (that form the first phase of MINE).

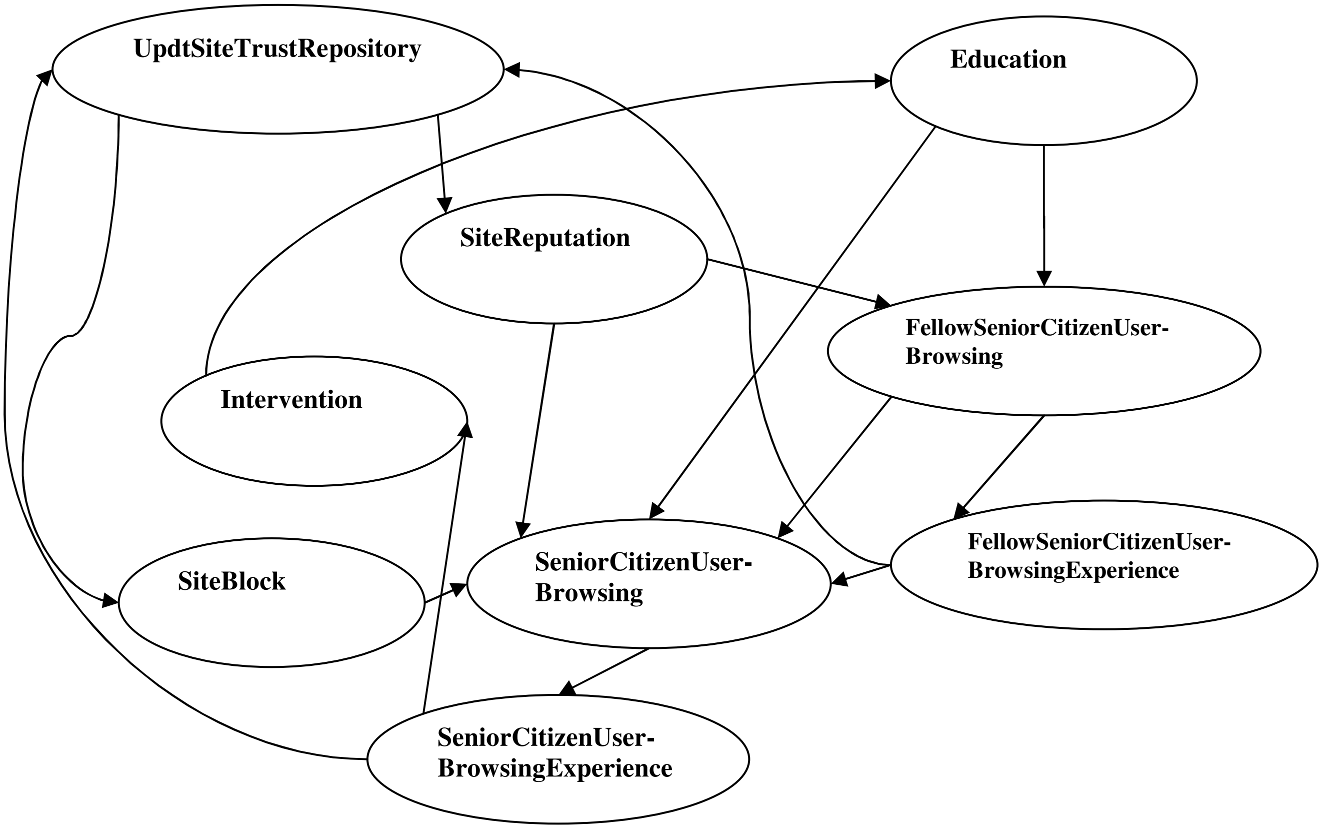
UpdtSiteTrustRepository
Education
SiteReputation
FellowSeniorCitizenUser-Browsing
Intervention
SiteBlock
SeniorCitizenUser-Browsing
FellowSeniorCitizenUser-BrowsingExperience
SeniorCitizenUser-BrowsingExperience

Figure 1. Bayesian Network Graph for SeniorCitizenUser belonging to Age Group 65-70

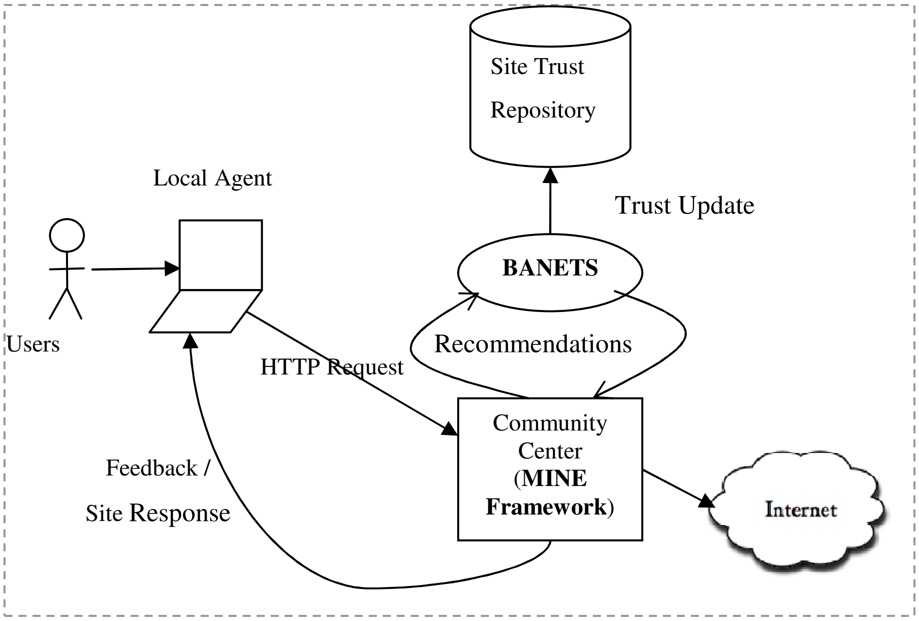

Figure 2. Conceptual Framework Design for Mediated Internet Experience

6. CONCLUSION

In this paper we have established the need to address online privacy issues of senior citizens who represent a very unique demography of Internet users in terms of several factors. We advocate a socio-technical approach that will begin with exhaustive survey and threat modeling, followed by appropriate training, education and induction into the MINE framework. Future work consists of more exhaustive graph modeling, condensing them for the sake of computational resource control and conducting appropriate surveys to categorize the seniors for the BANETS model and statistically determine the probabilistic quantities to help us run simulations for obtaining data before deployment. Finally, we intend to implement the MINE framework in community centers to evaluate its impact on senior citizens' browsing experience. The implementation of the trust gathering component will be a combination of software and possibly some hardware solutions with a distributed approach while the overall framework will be more centralized and implement algorithms like the one given above.

REFERENCES

[1] U. S. S. C. o. Aging, *Internet Fraud Hits Seniors: As Seniors Venture Into the Web, the Financial Predators Lurk and Take Aim*, 2004.

[2] P. Avesani, P. Massa and R. Tiella, *Moleskiing: a trust-aware decentralized recommender system*, 1st Workshop on Friend of a Friend, Social Networking and the Semantic Web. Galway, Ireland (2004).

[3] P. Avesani, P. Massa and R. Tiella, *A trust-enhanced recommender system application: Moleskiing*, *Proceedings of the 2005 ACM symposium on Applied computing*, ACM, Santa Fe, New Mexico, 2005.

[4] S. Fox, *Are "Wired Seniors" Sitting Ducks?*, *Pew Internet & American Life Project*, 2006.

[5] S. Ganeriwal and M. B. Srivastava, *Reputation-based framework for high integrity sensor networks*, Proceedings of the 2nd ACM workshop on Security of ad hoc and sensor networks (2004), pp. 66-77.

[6] A. Jøsang, R. Ismail and C. Boyd, *A survey of trust and reputation systems for online service provision*, Decision Support Systems, 43 (2007), pp. 618-644.

[7] L. Kwei-Jay, L. Haiyin, Y. Tao, C. Tai. and A. C.-e. Tai., *A reputation and trust management broker framework for Web applications*, in L. Haiyin, ed., *in the Proceedings of 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service, 2005. EEE '05.* , 2005, pp. 262-269.

[8] K. J. Lin, H. Lu, T. Yu and C. Tai, *A reputation and trust management broker framework for web applications*, International Conference on e-Technology, e-Commerce, and e-Services, pp. 262–269.

[9] M Chandrasekaran, M Baig, S Upadhyaya, *AVARE: aggregated vulnerability assessment and response against zero-day exploits*, Performance, Computing, and Communications Conference, 2006.

[10] W. Sears, Z. Yu and Y. Guan, *An Adaptive Reputation-based Trust Framework for Peer-to-Peer Applications*, Network Computing and Applications, Fourth IEEE International Symposium on (2005), pp. 13-20.

[11] N. Selwyn, *The information aged: A qualitative study of older adults' use of information and communications technology*, Journal of Aging Studies 18 (2004), pp. 369-384.

[12] B. M. Steve Sheng, Ponnurangam Kumaraguru, Alessandro Acquisti, Lorrie Faith Cranor, Jason Hong, Elizabeth Nunge, *Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish*, *Proceedings of the 3rd symposium on Usable privacy and security*, 2007.

[13] www.irs.gov, *IRS Warns of e-Mail Scam about Tax Refunds*, 2005.

[14] Z. Yu, W. Sears and Y. Guan, *PeerCredential: a reputation-based trust framework for Peer-to-Peer applications*, International Journal of Information and Computer Security, 1 (2007), pp. 256-277.

[15] Daryle Niedermayer, *An Introduction to Bayesian Networks and their Contemporary Applications*, http://www.niedermayer.ca/papers/bayesian/bayes.html, 1998.

[16] E Horvitz, J Breese, D Heckerman, D Hovel, K Rommelse, *The Lumiere Project: Bayesian User Modeling for Inferring the Goals and Needs of Software Users*, Microsoft Research, 1998.