Computer Viruses in Urban Indian Telecenters: Characterizing an Unsolved Problem

Prasanta Bhattacharya
Microsoft Research India
t-prabha@microsoft.com

William Thies
Microsoft Research India
thies@microsoft.com

ABSTRACT

Computer viruses can pose a serious threat to the operations of computer kiosks in the developing world. In this paper, we investigate the experiences, behaviors, and unmet needs of telecenter owners as they attempt to prevent virus infections on their machines. Based on interviews in 25 centers in Bangalore, India, we conclude that virus control is largely an unsolved problem for this population. We characterize the local strategies for coping with viruses, barriers to eliminating the problem, and opportunities for future research.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection—*Invasive software*; K.4.3 [**Computers and Society**]: Organizational Impacts

General Terms

Security, Human Factors

1. INTRODUCTION

Public-access, shared computing facilities play an important role in enabling low-income individuals to gain access to computers and the Internet. In India, it is estimated that there are over 180,000 cyber cafes and 40,000 Internet kiosks [5], and 37% of India's 22 million urban Internet users rely on cyber cafes for access [7]. While the social impact of such telecenters remains a subject of debate and active study [17], and there are many barriers to their success and sustainability in rural areas [3, 11], there is no question that public and shared-usage environments have become commonplace across many urban centers in the developing world.

In prior work on telecenters and shared-usage computing, there has been frequent anecdotal evidence that computer viruses represent a serious problem [1, 4, 6, 8, 20]. Shared computer centers are especially vulnerable to viruses due to usage of untrusted media (customer USB sticks), Internet browsing by untrained users, and limited human and financial resources for computer security. However, to the best of our knowledge, there has not yet been a methodical survey to assess the state of computer viruses in the developing world. Only by understanding real-world experiences with computer viruses, including the human processes that dictate virus detection and control, will it be possible to design new interventions that can be effective in practice.

In this paper, we survey the multi-faceted impact of computer viruses on shared-usage computing centers in urban India. Our focus is on private businesses that provide one or more computers for direct or intermediated use by customers. While this usually takes the form of a telecenter or cyber cafe, it also encompasses establishments such as mobile shops and photo studios. Our methods consist of semi-structured interviews with owners or employees of 25 shops.

Our findings re-affirm that computer viruses remain a serious problem for these organizations. More surprisingly, this problem persists despite 88% of the shops running antivirus software, and 73% of these installations being licensed with a paid subscription. We describe the diverse practices that have evolved to cope with computer viruses, spanning regular re-installation of the operating system to deliberate reduction of customers' privacy (curbing visits to "risky" adult websites). We also survey the barriers and constraints that inhibit better virus control, including the importance of customer convenience and technical misconceptions of shop owners. Finally, we close by outlining research opportunities that leverage these findings to enable new systems and protocols for overcoming the virus problem in developing regions.

2. RELATED WORK

There is a rich literature surrounding telecenters and public-access computing in the developing world. Despite considerable debate regarding their efficacy as a vehicle for social development, the impact of telecenters is not rigorously understood and remains an active area of study [17]. Researchers have examined the factors that contribute to the success and sustainability of telecenters in rural and small-town India [3, 9, 11]. While these studies point to the general demands of computer maintenance, they do not focus on the impact of computer viruses.

Most closely related to our work are the surveys of Internet cafes in urban and small-town India by Rangaswamy [15, 16]. This work probes the motivations and entrepreneurialism of the owners of 42 Internet cafes [15] and also highlights the grey market surrounding software and services in this setting [16]. However, there is no mention of computer viruses. Other researchers have focused on user behavior in urban Internet cafes, spanning overnight browsing in Nigeria [1], collaboration between users in Ghana [2], deliberate planning by users in Nairobi, Kenya [20], gaming in central Asia [10], and general usage patterns in urban India [6] and Kam-

NSDR'11, June 28, 2011, Bethesda, Maryland, USA.

pala, Uganda [13]. While these works contain occasional references to computer viruses, the issue is not explored in depth.

Broader research in the space of technology and development has grappled with the issues of computer viruses. Brewer et al. give anecdotes of virus infections and frequent re-installations of the OS in India and Cambodia, and suggest that antivirus software is rare in the latter environment [4]. Network traces from the village of Macha, Zambia show evidence of significant malware traffic [8]. Rahman et al. present an architecture for security and privacy of rural Internet kiosks [19]. As they utilize a Linux system, viruses are less common and their focus is on protecting user data.

Overall, despite the considerable interest in telecenters and Internet cafes, and widespread anecdotal evidence regarding computer viruses in developing regions, we are unaware of any systematic investigation into the experiences, challenges, and opportunities surrounding virus control in such environments. This provides the impetus for our study.

3. STUDY ENVIRONMENT

Our study was conducted via semi-structured interviews, performed by the first author over a period of 10 weeks in urban Bangalore. The focus was on small and medium-sized shops with one or more shared-access computers; we visited 25 locations in all. The target locations were selected via a convenient sampling, in which we visited three different neighborhoods in urban Bangalore (spanning lower- and middle-income communities) and searched for suitable businesses on the street. Interviews were usually with the owner or manager of the establishment, or (in 3 cases) with another employee. Interviews were conducted in Hindi and usually lasted between 45 minutes and an hour. As several interviewees were hesitant to be recorded while discussing software licensing and security, handwritten notes were taken during the interview and expanded shortly thereafter.

The vast majority of centers (23 out of 25) provide Internet access to the machines; 18 are set up as a cyber cafe for their primary business while 5 derive their primary income from other offerings such as mobile services, photo studios, design and printing, and computer sales and servicing. The two offline locations are primarily photocopy centers that also use computer kiosks for preparation and printing of documents. Across all locations, the most common use of computers is for preparing resumes and cover letters, and searching for jobs online. In addition, customers frequently use the computers to book tickets (for travel by train, bus, air, etc.), print documents, or for entertainment (playing games, accessing Facebook, etc.) Cyber cafes typically charge Rs. 10 ($0.22) per hour for access to the computers. Supplemental services such as printing are frequently responsible for a large share of the shops' revenue.

Most of the visitors to a given establishment are repeat customers, who are familiar with the shop and sometimes insist on using the same machine. Customers rely heavily on USB sticks to store their personal data across sessions. While they are discouraged from leaving persistent files on the computers in the shop, sometimes they do so by accident. By law, cyber cafes in India are required to maintain records of the identity of every customer. Consequently, several cafes have prominent signs asking customers to submit ID proof upon entry. However, these practices are rarely enforced in small shops. When asked about the sign requesting ID proof, one owner commented, “they are only for the authorities when they visit”.

Shops contained between 1 and 20 computers (median=7) as depicted in Figure 1, and had been using computers for a period of 3 months to 10 years (median=3). All shops were exclusively running Windows XP, with the exception of one medium-sized cyber cafe which was running Windows 2000 (motivated by the manager's belief that Windows 2000 was more secure with respect to viruses than Windows XP). One cyber cafe maintained a Linux machine, but only for use by the manager. We found only one instance of genuine Windows across the 25 locations. Respondents were amused when we asked about genuine Windows, with responses such as “I'm sure you have not come across a single cyber cafe that used a genuine copy of Windows” and “Who in today's world uses a genuine copy of Windows Sir?”

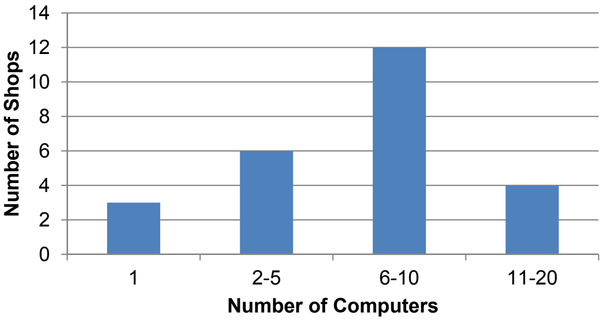

Figure 1: Number of computers in shops studied.

Maintenance and repair of computers is an ongoing challenge for all of the establishments that we visited. As detailed later, all shops make significant investments in controlling computer viruses: of 25 locations, 22 are running antivirus software and 16 are paying for licensed versions (often the only licensed software on the machine!). In addition, hardware failures are not uncommon, due in part to power fluctuations and outages. Most shops have made an arrangement with a computer repair person, who charges on a per-visit basis (approximately $5-$10) to come and re-install the OS. Larger cafes have annual maintenance contracts.

4. THE VIRUS PROBLEM

Computer viruses remain a significant problem in the environments studied. Viruses often have a serious impact on business productivity, both due to the direct toll on customers as well as the human and financial resources consumed in attempting to control and recover from viruses. Respondents attribute viruses as originating from customer USB sticks, in addition to Internet websites. Owners of mobile shops also cite SD cards as a frequent vector for virus infection.

The prevalence and impact of viruses is summarized in Figure 2. These results indicate respondents' answers to two questions, the first probing the incidence of virus problems in their shop and the second inquiring as to the overall impact of those problems on their business. Answers were provided in free-form conversation and subsequently coded by the researcher. As evident in the figure, 80% of centers experience moderate to high prevalence of computer viruses, where “moderate” indicates regular infections that cause considerable problems and “high” corresponds to continuous, highly detrimental infections. The impact on daily business operations is also significant, with approximately one third of respondents indicating moderate impact (noticeable decrease in daily business, loss of direct revenue and customers' good will) and the same fraction indicating high impact (major threat to health of business, severely impacting daily productivity levels).

Interestingly, virus problems persist despite strong awareness of the problem, as well as extensive usage and investment in antivirus software. Figure 2 also summarizes the average expense on

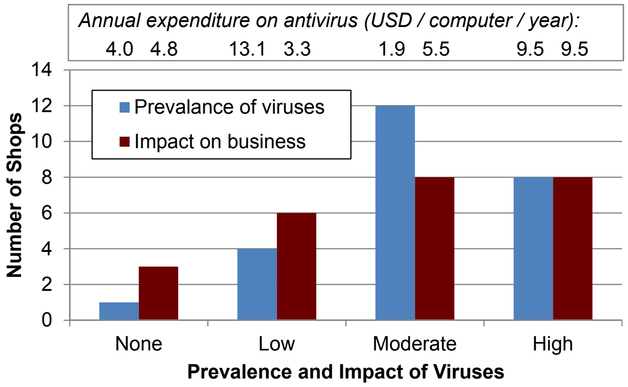

Figure 2: Prevalence and impact of computer viruses in shared-usage environments. The table at top summarizes the amount spent on antivirus software, for each center represented in a given column.

antivirus software, grouped according to the severity of the virus problem in a given location. While the expenses on antivirus software are highly variable (for reasons detailed in the next section), it is evident that investment in antivirus software is not sufficient to spare a shop owner from the problems described above. Those centers that lack antivirus software (N=3) or have only an unlicensed version (N=5) observe moderate (N=7) or high (N=1) incidence of viruses. However, the impact of those viruses on the business is spread equally from low to high.

We gathered numerous anecdotes that illustrate the severity of the virus problem for this population. For example, the manager of a photo studio related to us:

> An entire marriage ceremony tape got ruined at one time. All the audio and video files suddenly changed type into an unknown format and wouldn't open in any existing player. The customer ended up losing all the precious data from the ceremony, and was really furious about it.

This individual runs a registered version of QuickHeal antivirus (one of the leading solutions in India). He attributes the problem to outdated virus definitions. Due to this issue, he has shifted back to his old VHS camcorder to cover all major events such as weddings.

Virus problems can also have a direct economic impact on the business, as customers demand compensation for lost data. For example, the owner of a cyber cafe told us:

> The biggest problem was with a customer whose pen drive got corrupted due to some virus in my system. Even though the files were still in the drive, we couldn't see or access them. It was a big problem for us. We had to take the drive to a shop in Jayanagar [a distant location] for data recovery and spent some 2000 rupees [$45] on it. We used to frequently visit that shop for data recovery those days.

Sometimes the goal of preserving customer data stands at odds with protecting the security of the system. For example, the owner of a small photocopy center recounted:

> The problem with my antivirus is that when I scan my computer, if it finds an infected file, instead of removing the virus, it ends up removing the whole file. Twice, important customer data has got lost due to this scanning process. Hence, I ignore all such alert messages.

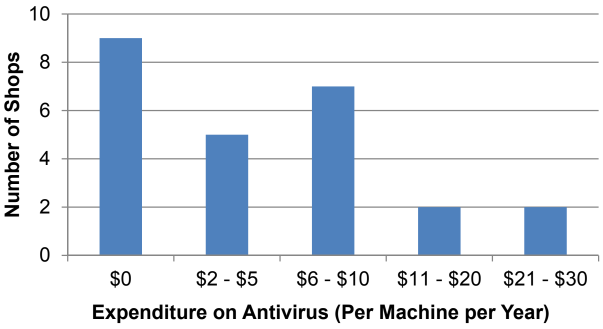

Figure 3: Expenditure of centers on antivirus software.

In addition to losing customer data, viruses commonly impact businesses by causing machines to crash or become unusably slow. Due to the magnitude of the virus problem, shop owners have developed numerous techniques to try to manage the situation, as we describe in the next section.

5. COPING WITH VIRUSES

In this section we describe the current practices employed by shop owners in response to the threat of computer viruses. While some are standard (such as usage of antivirus software), others are innovative socio-technical protocols that grew organically out of this environment. We contend that it is important to understand the strengths and limitations of these approaches, as together they have yet to arrive at a satisfactory solution to the problem. Also, some practices are quite laborious (such as re-installing the OS) and could perhaps be addressed by future technology interventions.

5.1 Antivirus Software

All but 3 of the 25 sites utilized antivirus software of some form. A variety of antivirus software was employed, and sometimes multiple brands in one location. The most popular were Kaspersky (N=9), QuickHeal (N=6), and Avast (N=4). Also represented were McAfee (N=3), Avira (N=3), Norton (N=2), AVG (N=2) and Xoft-Spy (N=1). (We discuss usage of rollback software such as Deep Freeze separately, in Section 5.3.) It bears noting that QuickHeal, though less common on a global scale, is based in India and is one of the most popular antivirus packages in the country. The majority of respondents initiated a virus scan on a daily basis, while a smaller fraction performed manual scans on a weekly or monthly basis; however, we do not emphasize this data as we believe that most scans were initiated automatically by the antivirus.

Given that it is rare to find authentic, licensed software in cyber cafes (see Section 3), we were surprised that most businesses are paying for licensed versions of the antivirus software. The costs are illustrated in Figure 3. It is evident that the costs are highly variable, owing primarily to the fact that different owners utilize each licensed copy on a different number of machines. In one case, the owner of a large cyber cafe maintains QuickHeal on only one machine, but uses it to scan the drives of all 20 machines over the network. Thus the cost incurred to him is only $4 per computer, which is over 7 times cheaper than another QuickHeal user that we interviewed. Nine shops show an antivirus expenditure of zero; these fall into three categories: 1) there is no antivirus in use (N=3), 2) there is an antivirus but it is cracked (unlicensed) and potentially obsolete (N=4), and 3) the antivirus is a time-limited trial version (N=2). In one case, a magazine store owner continually re-installs the latest trial versions, which he extracts from the magazines in his store.

5.2 Re-Installation of the Operating System

Due to the difficulties of controlling viruses on shared-access computers, many shop owners frequently revert to performing a fresh installation of the entire operating system. There is a perception that virus control is infeasible in a shared-usage environment, thereby leading to this solution. For example, the owner of a cyber cafe with six computers notes:

> Antiviruses are ideal for home use. For cyber cafes, it is better to dust, clean and format the systems once in a while, to keep them safe.

We inquired as to the frequency with which businesses resort to wiping and re-installing the operating system. Results appear in Figure 4. It is evident that this practice is quite frequent; the average period between re-installs is 5 months, with 5 respondents re-installing once per month and 6 respondents reinstalling once every 2-3 months. The re-installation is typically done by a computer helper or repair person who brings the requisite software (a pirated copy) and charges $5-$10 per visit. This implies that for many locations, the cost of re-installing the OS exceeds that of the antivirus software.

5.3 Rollback Software

Given the desire to safely restore machines to a prior state in shared-usage environments, several companies have designed rollback and recovery software for exactly this purpose. For example, systems such as Deep Freeze and Returnil allow the administrator to "freeze" the machine, implying that all changes imparted by a user will be discarded upon reboot. If the administrator wants to make permanent changes to a machine, he can do so by entering a password-protected admin mode. (We discuss limitations and extensions of this idea in Section 7.2).

We encountered four installations of Deep Freeze amongst our sample set. However, three were inactive, and one was apparently not helping to control the virus problem in the store. In the last case, the owner of the store (a cyber cafe with 14 computers) remarked to us:

> Oh, Deep Freeze does not get rid of your virus problems. I kept having these viruses, due to unsafe browsing, due to which I finally got myself an antivirus.

While this individual had previously demonstrated a basic understanding of Deep Freeze's functionality, this quote represents a misunderstanding regarding the usage of the software. If the machine became infested with viruses, it should be easy to fix with a reboot. We hypothesize that the machines in this location became infected when Deep Freeze was running in administrator mode, as owners had difficulty understanding how to enter and exit administrator mode at the right times. Due to this issue, rollback software such as Deep Freeze could actually worsen the situation, as a virus obtained in administrator mode would be impossible to remove from user mode (the virus would be "restored" on every reboot).

Overall, our conversations with current and former users of Deep Freeze indicated a conceptual gap regarding the capabilities of the software. The respondents strongly associated the notion of "antivirus" with actively "scanning" the system, something that is impossible to do using Deep Freeze or similar rollback software. Thus they gave up on the software without necessarily understanding its benefits and limitations.

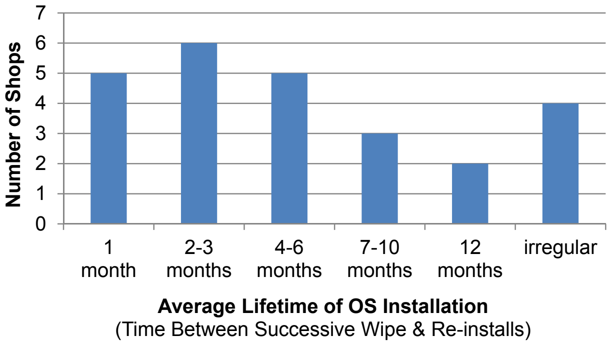

Figure 4: Usable lifetime of a computer before requiring a fresh installation of the operating system. Figures apply to a single machine; a shop with many machines performs re-installations much more frequently.

Such usability barriers represent a sobering example of how the most "simple" and "natural" software is not necessarily the most automatic; rather, it is the one that matches most closely with the user's existing mental model of the problem domain. We hypothesize that including a "scan" button in a rollback client – even if implemented via a reboot – would improve the uptake of the software.

5.4 Content Control

As many computer viruses originate from pornographic websites, several shop owners have taken steps to control the content that is viewed from their computers. The owner of a medium-sized cyber cafe described how he intentionally reduced customers' privacy in an effort to control computer viruses:

> Earlier, there were a lot of customers who used to frequent my shop in the evenings to visit pornographic sites. Those days, at least one system used to go down every single day, and I had to format the machine in the mornings. Then I turned the systems to face me, and they stopped coming.

In a similar vein, another cyber cafe owner described his plans to move his photocopier to face the computers, so he can better supervise activity there. In two locations, school-aged kids are required to come with their parents to prevent misuse of the machines. Several shops also contain prominent signs that prohibit viewing pornographic content.

Besides pornography, other kinds of activities have been perceived to correlate with viruses in the shops, and the corresponding behaviors are disallowed due to virus concerns. For example, the owner of a cyber cafe with 13 computers remarked:

> We also allowed a few systems to be used for gaming, but noticed a rise in viruses in those systems. We have stopped allotting machines for gaming ever since.

We did not establish whether there was actually a correspondence between gaming and viruses. Sites hosting cracked games could be a source of viruses, or perhaps the gamer demographic is more likely to admit other viruses.

5.5 Human Vigilance

We encountered several instances where shop owners are very vigilant about preventing unchecked storage devices from being inserted into shared computers. An owner of a cyber cafe devotes an entire machine to scanning users' USB drives; the drives must be scanned there prior to use in any other machine. An owner of a mobile shop completely prohibits users from inserting their SD cards into shared hardware. In case they want to download content from his shop, they also have to buy a fresh SD card on the premises. While these practices are deemed important for virus control, unfortunately both locations are still suffering from viruses due to other sources, presumably the Internet.

6. BARRIERS TO VIRUS CONTROL

To better inform research that seeks to improve virus control in shared-usage environments, we outline a number of constraints that any new solutions will have to overcome.

6.1 Customers Must Not be Inconvenienced

While many owners are aware that viruses could be controlled better if every customer's personal USB drives were subjected to strict scanning protocols, they were dismissive of this idea due to the potential burden on customers. For example, the owner of a cyber cafe with six computers stated:

> I cannot enforce any such strategy or policy as that might end up troubling the customers. If a customer brings an infected disk/drive, I really don't have an option.

When pressed as to whether he at least asks customers to scan their drives prior to opening a file, he replies: "No, I cannot afford to. Customers do not seem to have the time."

The same philosophy restricts the adoption of new technologies, including operating systems. While the owner above administers his own Linux box with no virus difficulties, he says that customers would not find the interface to be usable. Other owners have cited similar familiarity and usability concerns as a reason for not upgrading the operating system (e.g., from Windows 2000 to Windows Vista) even when they understood that the latter had better security properties.

6.2 Misconceptions of Shop Owners

Another barrier to the adoption of new technologies is the education and awareness of shop owners. Illustrated previously for the case of rollback and recovery software, there are frequent misconceptions that have a direct bearing on virus control. For example, an owner of a small shop (with just one computer) was convinced that infections from the Internet were no longer possible on his machine, as the vendor had blocked all suspicious sites. Many owners remain pessimistic (and perhaps with some justification) regarding the potential of new technologies, citing that "there's little we can do" against certain viruses and viruses such as "Autorun" present "no alternative than to format the entire system". Finally, the owner of one Internet cafe was convinced that computer viruses represent a conspiracy on the part of antivirus companies, who develop and disseminate viruses to promote their own products.

7. RESEARCH OPPORTUNITIES

Based on our findings, we outline directions for future research that could have a beneficial impact on the management of computer viruses in shared-usage environments.

7.1 An Epidemiology of Computer Viruses

One of the most intriguing aspects of our results is that many shops remain riddled by viruses despite the installation of up-to-date, state-of-the-art antivirus software. Which viruses are responsible for these infections, and why are they not being detected? This question is especially interesting in offline environments, where the primary vector of virus transmission is USB sticks rather than Internet websites.

We envision a rich scope to perform an "epidemiology" of the computer viruses affecting developing regions, to better understand the prevalence and transmission of certain kinds of viruses. Analogous to a medical epidemiology, are there specific viruses that are responsible for most of the problems in computer health? Are these new viruses that are affecting machines on a global scale, or are they old viruses that have been "eradicated" in rich countries? Are there specific, targeted interventions (such as a virus signature sent via SMS to offline locations) that can prevent the spread of such viruses, or quickly "cure" an outbreak when they occur? An innovative approach for conducting such an epidemiology was developed in tandem with this research [14].

7.2 Improve Rollback and Recovery Software

We believe that there is a large opportunity to improve rollback and recovery software (similar to Deep Freeze) for users in developing regions. Currently, the available offerings have several limitations. First, the user interface and mental model is a mismatch for users, preventing their uptake even in cases where they may be effective (see Section 5.3). Second, they have not been designed for the constraints of developing regions. For example, Deep Freeze assumes that users' sessions are never interrupted by a power-down event; if there is a power outage, Deep Freeze would discard all temporary files belonging to a user! Finally, existing rollback and recovery software relies on buffering writes to disk, a mechanism which viruses can subvert by installing their own disk driver [12]. This vulnerability recently led to the compromise of over 45,000 public-access computers in Asia, due to a worm called SafeSys [18].

To address these shortcomings, we originally envisioned an approach based on virtualization. By using off-the-shelf virtualization software, one could create isolated environments with flexible rollback and recovery options. We pursued this idea by building a simple user interface on top of a virtual machine, forcing owners to choose between administrator mode (changes are saved) and user mode (changers are discarded) upon every boot. However, when we deployed this system in an Internet cafe, we discovered that owners were not willing to tolerate the delay of loading a virtual machine (about 5 minutes on their slightly outdated hardware) after every boot. A general-purpose virtual machine may also pose challenges to steady-state performance and compatibility with older systems.

Based on this experience, our current interest is in using lightweight disk imaging software to provide a robust and flexible rollback mechanism. Disk images are used by both virtual machines and backup systems to encapsulate the complete state of a hard disk. As such, they can be used to clone the entire working environment of a shared machine, and to revert to a prior copy in the event of virus infection. However, to date the available user interfaces for disk imaging are highly specialized and not suitable for routine use by novices. We envision a system whereby at least two copies of an image are maintained at all times; one is used as a sandbox for the current session, while the other provides a stable backup. The backup can be restored either on a regular basis, or as needed to cope with viruses.

7.3 Leverage Relaxed Privacy Norms

Relative to rich countries, in the Indian context there is often a looser expectation of privacy in interacting with technology; many experiences of technology are shared amongst onlookers. Given that there is frequently a tradeoff between security and privacy, it could be possible to leverage this cultural norm in new ways to improve the security of computer systems. One example of this is the deliberate re-arrangement of a cyber cafe to reduce pornographic content by decreasing privacy (see Section 5.4). Other owners that we spoke to expressed similar sentiments, for example:

> I think too much of privacy given to the users is not good. We should monitor the customers to a certain extent.

While we have not designed specific interventions in this vein, there could be several possibilities. For example, installation of lossy screen recorders (which mask personal details such as credit card numbers, but enable shop owners to monitor one's overall task) could incentivize users to be careful online without violating their expectations of privacy.

7.4 Leverage Willingness to Pay

One of the most striking outcomes of our survey is that shop owners remain unsatisfied with the available solutions for virus control, and in fact, they are willing to pay more money in exchange for a better experience. When asked explicitly whether they were willing to pay more for a better antivirus, 21 out of 25 respondents answered affirmatively. For example, one of them said:

> I'm sure all studios like us wouldn't mind in spending an additional 500-1000 rupees [$11 - $22] on a much better antivirus software. [...] Even though all major antivirus providers make tall claims, none of them are actually significantly useful in tackling the issue.

Perhaps one manner in which to respond to this demand would be to provide enhanced services in addition to the technology, for example, subscription-based training as to what best practices should be followed in a shared usage environment, or suggestions on human processes (such as scanning USB sticks) that can improve the virus situation. It may also be possible to leverage this willingness to pay in order to overcome the traditional barriers facing challenged environments, for example, to provide updated virus definitions via postal mail rather than over the Internet.

8. CONCLUSIONS

This paper represents an exploratory study of the impact of computer viruses on shared-access kiosks in urban India. We confirm anecdotal evidence regarding the severity of the virus problem, and document that the problem persists even when licensed antivirus software is employed. We describe organic techniques that have developed to cope with the problem, including regularly wiping and re-installing the operating system as well as restricting the content accessible to users. We illustrate social barriers, such as hesitancy to inconvenience the customer and limited education of the owners, that could prevent a purely technical solution from taking hold. Finally, we offer directions for future research that could potentially make new headway.

One limitation of our study in its current form is the relatively small sample size (25 locations). Incorporating a larger sample would enable us to improve the external validity of the findings, and also to examine the correlation between specific factors, such as the size of the shop or the education of the owner, with the prevalence of computer viruses.

9. ACKNOWLEDGMENTS

We thank Saurabh Panjwani and Nimmi Rangaswamy for providing helpful feedback on prior drafts of this paper. We are also indebted to our respondents for their kind participation in our study.

10. REFERENCES

[1] E. Adomi. Overnight Internet Browsing Among Cyber Café Users in Abraka, Nigeria. *Journal of Community Informatics*, 3(2), 2007.

[2] M. Best. Connecting In Real Space: How People Share Knowledge and Technologies in Cybercafés. *AMIC Annual Conference*, 2010.

[3] M. Best and R. Kumar. Sustainability Failures of Rural Telecenters: Challenges from the Sustainable Access in Rural India (SARI) Project. *Information Technologies and International Development*, 4(4), 2008.

[4] E. Brewer, M. Demmer, M. Ho, R. Honicky, J. Pal, M. Plauche, and S. Surana. The Challenges of Technology Research for Developing Regions. *IEEE Pervasive Computing*, 5(2), Apr. 2006.

[5] Cyber Cafe Association of India. `http://www.ccaoi.in/UI/links/cms.php?id=19`, 2009.

[6] A. Haseloff. Cybercafes and their Potential as Community Development Tools in India. *Journal of Community Informatics*, 1(3), 2005.

[7] I-Cube 2009-2010 Internet in India. `http://www.imrbint.com/index.php?id=1`, Feb. 2010.

[8] D. Johnson, V. Pejovic, E. Belding, and G. van Stam. Traffic Characterization and Internet Usage in Rural Africa. In *WWW*, 2011.

[9] J. Kendall and N. Singh. Internet Kiosks in Rural India: What Influences Success? *NET Institute Working Paper*, 06-05, 2006.

[10] B. Kolko and C. Putnam. Computer Games in the Developing World: The Value of Non-Instrumental Engagement with ICTs, or Taking Play Seriously. In *ICTD*, 2009.

[11] R. Kuriyan and K. Toyama. Review of Research on Rural PC Kiosks. `http://research.microsoft.com/research/tem/kiosks`, 2007.

[12] Wilders Security Forums. Virtualization/rollback software test. `http://www.wilderssecurity.com/showthread.php?t=276210`, 2009.

[13] P. Mwesige. Cyber elites: a survey of Internet Café users in Uganda. *Telematics and Informatics*, 21(1), Feb. 2004.

[14] M. Paik. Gotta Catch 'Em All! Innoculous: Enabling Epidemiology of Computer Viruses in the Developing World. In *NSDR*, 2011.

[15] N. Rangaswamy. Telecenters and Internet Cafés: The Case of ICTs in Small Businesses. *Asian Journal of Communication*, 18(4), 2008.

[16] N. Rangaswamy. The non-formal business of cyber cafés: a case-study from India. *Journal of Information, Communication and Ethics in Society*, 7(2/3), 2009.

[17] A. Sey and M. Fellows. Loose strands: searching for evidence of public access ICT impact on development. In *Proceedings of the iConference*, 2011.

[18] SPAMfighter News. BKIS - Deep Freeze Application Fails to Detect New Chinese Worm, June 2009.

[19] S. Ur Rahman, U. Hengartner, U. Ismail, and S. Keshav. Practical Security for Rural Internet Kiosks. *NSDR*, 2008.

[20] S. Wyche, T. Smyth, M. Chetty, P. Aoki, and R. Grinter. Deliberate interactions: characterizing technology use in Nairobi, Kenya. In *CHI*, 2010.