Computing Security in the Developing World: A Case for Multidisciplinary Research

Yahel Ben-David,[*†] Shaddi Hasan,[*] Joyojeet Pal,[‡]
Matthias Vallentin,[*] Saurabh Panjwani,[§] Philipp Gutheim,[*] Jay Chen,[¶] Eric Brewer[*†]

Abstract

Technology users in the developing world face a varied and complex set of computer security concerns. These challenges are deeply tied to a range of contextual factors including poor infrastructure, non-traditional usage patterns, and different attitudes towards security, which make simply importing security solutions from industrialized nations inadequate. Recognizing this, we describe some of the specific security risks in developing regions and their relationships with technical, political, social, and economic factors. We present concrete examples of how these factors affect the security of individuals, groups, and key applications such as mobile banking. Our analysis highlights the urgency of the concerns that need attention and presents an important intellectual challenge for the research community.

1 Introduction

Computing security is an important concern for researchers working on issues of technology and development. From casual concerns about viruses in email or infections via USB key drives used in cybercafes, to serious issues with identity theft on shared networks, computing security poses a diverse set of challenges.

Although we do not argue that the threat in the developing world is necessarily *greater* than elsewhere, we do find that security issues in the developing world are *different*, and as such are underrepresented in research and practice. We argue the poor security situation is not simply due to a lack of technical tools: the root causes stem from a combination of technical and non-technical issues, and thus require a multidisciplinary approach for solution design. Examining these problems is not only valuable in providing a more secure computing environment in the developing world, but also holds the potential to re-examine issues of mainstream security studies, given the diversity of computing environments, networks, and risk behaviors.

Rapid economic growth and increasing technology usage, coupled with the continued existence of the five forces described in the next section, create a security landscape where attackers have both the incentive and the ability to inflict significant harm to technology users. This hypothesis is supported by evidence from the computer security world: the Norton CyberCrime Report attempts to quantify the time and money for recovery from cybercrime across 14 countries [1]. Juxtaposing these results with GDP reveals that these costs form a much higher percentage of GDP for developing countries (i.e., Brazil, China, India). We can also use proliferation of botnets as a metric for the impact of poor security, and again we see that India, Russia and Brazil are top sources of spam, with China being on par with the USA [2]. Similarly, we see that Brazil (10.5%), India (9.3%), Russia (7%), the USA (5.8%), and China (5.1%) lead the global botnet activity for dictionary attacks [3].

Aside from these measurable impacts of security issues, the indirect impact of poor security is equally damaging. In particular, compromised computing infrastructure is often unreliable and can negatively affect the confidence placed in technology rather than fostering its adoption. We observed this distrust in technology ourselves as part of our experiences with computer users in India. As a result, we formulate two hypotheses.

Developmental Impact: There is significant evidence that poor security practices prevail in the developing world, yet the extent to which this hinders development is unknown. Indeed, understanding the impact of poor security practices is challenging since often it is not manifested directly. Beyond the direct cost to consumers and indirect effects on technology adoption, we suspect poor security prevents technology-based development from achieving its full potential.

Risk: The second open issue is the relative level of risk in developing regions, where we define risk as the probability of being exploited multiplied by the cost of a security breach. The probability of exploitation is a function of both the quality of security practices and the incentives for

[*]University of California Berkeley.
[†]Also AirJaldi - Dharamsala, H.P., India
[‡]University of Michigan, Ann Arbor.
[§]Microsoft Research India.
[¶]New York University.

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

attack. Although users in developed countries tend to have more resources for defending their computing environment, they also present a more lucrative target, due to higher incomes and more powerful computing infrastructure. The relationship among these factors is complex and we expect that there exist environments where all three (ability to defend, incentives for attackers, and impact of exploitation) are aligned to promote attacks. It seems likely that novice middle-income users, a large and growing group, are both easy to reach and worth attacking.

2 Security Landscape

In exploring this space, we identify five core forces that shape the security landscape in the developing world. We discuss the potential developmental impact they imply, and propose a multidisciplinary research agenda towards addressing the broad range of challenges.

2.1 Poor Security Hygiene

A key factor in assessing the security of a system is its "security hygiene", i.e., the degree to which it runs with up-to-date software patches and recent malware protection. For example, systems with a high security hygiene regularly update their operating system and anti-virus software, have recent versions of security-critical components such as Flash or Java, and employ browsing blacklists (e.g., Google Safe Browsing). The concept of security hygiene also applies to the firmware of embedded devices, such as wireless routers. Naturally, systems with high security hygiene exhibit a smaller attack surface and therefore face fewer potential hazards.

Security hygiene in the developing world is generally poor. For example, one study found only 30-40% of systems in the AirJaldi [4] network performed anti-virus and OS updates [5]; another study of an Indian telecenter found high infection rates and wasted bandwidth due to Portuguese spam [6]. One of the reasons for this situation is the fact that Internet access in the developing world is characterized by scarce bandwidth and frequent failures. Even when an individual connection is fully operational, end-to-end traffic flows are subject to bottlenecks at upstream links or high packet loss rates.

These network conditions make obtaining security updates, patches, and malware signatures (which often require regular and lengthy downloads) a tedious and failure-prone process. The combination of slow download speeds with frequent failures and congestion often leads to failed downloads that need to be attempted again, leading to a self-reinforcing state of poor performance that is difficult to escape, and which may ultimately have detrimental effects on the security hygiene. Indeed, Maier et al. [5] find that the fraction of OS and anti-virus updates of the total HTTP traffic is larger in the AirJaldi network compared to the large European ISP, which could be explained by the intermittent connectivity that causes more updates to fail. To support this hypothesis, we analyze the TCP state of connections to `windowsupdate.com` and `update.microsoft.com` in the AirJaldi network and compare it to two research sites in Berkeley, California: the Lawrence Berkeley National Laboratory (LBNL) with more than 12,000 hosts, and the International Computer Science Institute (ICSI). Comparing connection logs from the whole month of February 2011, we find that 56% of all Windows Update connections at AirJaldi are terminated with a RST by the originator, indicating a failed update attempt. This is an order of magnitude higher than for ICSI and LBNL.

In industrialized nations, bandwidth is often seen as a commodity with relatively small cost. Not surprisingly, operating systems, software, and security applications alike take it for granted that patches and updates for their products will be delivered to clients online. With the prevalence of risk that is promulgated online, and given the near ubiquity of reliable Internet in the primary markets of software producers, this is arguably the most practical means of providing updates. However, the assumption of easily-available, inexpensive, and reliable connectivity does not necessarily hold in the developing world, and may even be counter-productive as a security practice.

Further complicating this view of security hygiene is the fact that many types of malware spread without any online connectivity. Offline infection vectors such as USB storage devices have been shown to be very effective and often harder to protect against [7]; the disinfection and cleaning processes are significantly more complex without Internet access. These attack vectors can be very unexpected. For instance, while surveying rural branch offices of an NGO in Rajasthan, India, one of the authors found several offline PCs running Windows XP which had been infected with viruses. Apparently, the viruses were reaching these machines via memory cards of digital cameras used by the NGO for fieldwork: there were very few external backup devices in these offices, but up to 70 memory cards were floating in circulation per office (for less than 15 PCs) Interestingly, the NGO reported that mainstream anti-virus programs, which offered adequate security in their Internet-connected urban offices, could not fend off all viruses in these rural locations.

2.2 Unique Usage Patterns

The unique resource constraints faced by technology users in the developing world has given rise to new computing environments and applications not commonly seen in the developed world. For example, people in developing regions are beginning to rely on mobile technology for conducting financial transactions even in places where credit cards and the web have not penetrated. The M-Pesa service in Kenya and its numerous clones throughout the developing world [8] enable people to manage savings accounts, make electronic payments and now even avail themselves of loans and micro-insurance [9]. Some of these services have recorded daily transaction volumes of over hundreds of millions of dollars [8].

Although these services are not new, the security of the underlying technology is poorly understood: unlike ATMs and credit cards in the West, there are no industry standards for building secure mobile banking technology; in fact, at least three such services have been successfully attacked in different ways in the past year alone [10, 11, 12]. The core

challenge in designing secure solutions for this application stems from the fact that a majority of the phones available in developing regions are still of a very basic nature: they are either not programmable at all or offer only limited programming capability. This makes it difficult to adapt security solutions designed for other forms of electronic commerce into the current context, and practitioners are forced to resort to ad-hoc approaches, as done in current deployments. The situation is further complicated by the fact that these systems have been shoehorned on top of the GSM signaling channel (using protocols like SMS or USSD) which were never designed or intended to facilitate secure transactions. Given the increasing penetration of such services and the recent spate of attacks against them, it is of urgent importance that security researchers come up with an innovative remedy for this situation.

Another source of security concerns is shared resource computing. PCs in developing countries are predominantly a shared resource [13]. Most families do not own a PC and therefore use cybercafes, kiosks and community centers where PCs are shared with others. Extensive literature exists regarding the risks involved with the use of public terminals, as well as suggestions for mitigating these problems [14]. Although the use of public computers in the West is diminishing — and with it academic interest from computer scientists — securing this type of computing environment remains a common challenge in the developing world. Additionally, differences in elements such as purchasing power, literacy levels, and maturity of privacy and identity concepts may render existing solutions ill-suited to rural developing regions. There is much literature on the prevalence of both outgoing security threats through phishing activity and virus infection of individual machines in cybercafes and shared computer centers [15]. Shared machines at computer centers suffer from a "tragedy of the commons" scenario with regard to security, because individual users have no real incentive to keep the devices safe for other users. At the same time users at cybercafes are frequently driven by what may be termed as risky activities, such as pornography or online gaming [16]. A cybercafe manager who denies such services to his or her clientele risks losing customers. Shared computer centers are often the primary location not just for Internet access, but also general computer access. Users typically use the machines for a range of activities, like desktop publishing or writing a resume, for which they frequently use external USB storage. These are frequently infected, and given that for many users the storage is the only computing artifact they actually own, they carry the infection wherever they go. As with censorship, prohibiting USB keys is often not a viable business decision.

2.3 Novice Users

According to the World Bank[17], more than half of the Internet users in low and middle income countries have joined since 2005; the number of users in these countries has increased by over 190 million between 2007 and 2008 alone. Despite the obvious need, disseminating security educational material and tools is extremely challenging. Many of these users have their first experience with the Internet on a mobile device, a platform with its own unique security implications. A general lack of language support and localization of applications and technical instructional material can undermine user awareness of security risks. Content in the online environment is primarily in English and Chinese, further complicating the situation for the many users not literate in these languages.

Inexperienced users may exhibit a variety of behaviors that may adversely impact security, such as engaging in risky online behavior [18] or forwarding emails from questionable sources. While there is little existing work on the comfort of users with potential attack vectors such as pop-ups, online adware, or installing untrusted software, there has been some work on the spread of viruses through email. The damage caused by email-based virus spreading has been an important area of work in both engineering [19] and economic studies [20] in terms of the cost of such activities to individual productivity and to the network [21]. There have also been studies examining the motivations of people in forwarding emails [22, 23], though there is little structured empirical knowledge on the demographics of "potentially unsafe" email behavior [24]. Though there are significant variances in data, the general trend seems to suggest that there is a greater likelihood of email infection in the developing world, especially in China and India. The MessageLabs network infection report [25] finds that India and China are both leading sources as well as intended destinations of attacks.

Several news and marketing reports discuss the incidence of phishing and the consequent lack of user trust on Internet-based activity in India. A survey commissioned by VeriSign revealed that at least 76% of the web users in India are at risk from online fraud due to the inability to identify different forms of phishing. Recognizing the potential biases of marketing research, this data nonetheless suggests that low user awareness of security issues increases risk. Although there is no conclusive evidence that cultural factors make the developing world more susceptible to phishing, there is plenty of research that shows cultural differences in online behavior and purchasing practices [26]. Research at Symantec, for instance, showed that spammers and creators of malicious software are both aware of user behavior issues and target these specifically in their effort to expand botnets by exploiting religious festivals, such as Diwali in India [27]. Attitudes towards potentially dangerous online material also appear to vary by region. One study found that despite higher use of anti-virus software, users in rural India tend to click on Google search results that are clearly marked as dangerous and which most European users avoided [5]. Given the large influx of novice users, these issues remain a significant cause for concern.

2.4 Piracy

Our experience suggests that most proprietary software in use throughout the developing world is pirated. While use of pirated software is not necessarily a security risk, it is challenging to verify that such software is not malicious. Pirated operating system disk images, for instance, are difficult to scan due to their size; additionally malware can be

easily hidden from the user once the operating system itself is compromised.

Moreover, verifying the source of pirated software is impossible, and the motivations of the creators of such pirated software are unclear. The pirated operating system distributions the authors came across clearly required a non-trivial amount of work to produce, and many even include a variety of additional (pirated) application software pre-configured and ready to use. Despite this, the proliferation of these all-in-one pirated images makes some forms of recovery from infection easier: users simply re-image their machines when they have been compromised. As data loss is almost expected, the practical cost to re-image for recovery is low.

Use of pirated software also appears to decrease security hygiene. Older versions of pirated software are generally considered easier to obtain in the gray market; this is especially true for Windows XP, first released in 2001, compared to more recent versions of Windows [28]. Additionally, software vendors take measures to protect against software piracy, and while mostly unsuccessful it is far easier to confirm the authenticity of software when it requests security updates. As expected, many pirated copies cannot obtain security patches and are therefore left vulnerable to attacks. Since companies like Microsoft monitor computers making online requests for updates, users who are concerned about the legal implications of piracy may voluntarily avoid the update process.

The proliferation of pirated software is a multifaceted phenomenon. Despite a negative relationship between software piracy rates and economic development, software piracy cannot be explained by economic factors alone — a range of policy and cultural issues also plays a role [29, 30]. Legacies of weak regulatory controls and the network effects of widespread piracy contribute to a casual attitude towards piracy [31]. For many countries, the regulation of piracy is politically sensitive as it ties in with a range of other trade issues [32]. A tangentially related concern is the widespread piracy of music and movies, which often involve quasi-legal websites [33]. Both the content and the websites themselves are likely to pose malware risks. Because the regulatory and enforcement environments are unlikely to change dramatically within the next few years, piracy will likely continue to influence the security landscape.

One possible means of mitigating the security risk of pirated software is increasing awareness of open-source alternatives to popular software, which are generally less often targeted for attack than proprietary alternatives, if not actually more secure. As the authenticity of open source software can be easily verified, the risk of "pre-compromised" software from unknown, potentially malicious sources is dramatically reduced. Open source software can be easily bundled together for distribution, much like the all-in-one bundles of pre-configured pirated software currently in circulation; thus users can continue to enjoy the benefits of quick, low-cost recovery currently provided by all-in-one pirated software distributions without the associated risks.

2.5 Adversaries' Perspectives

An attacker's motivations for compromising a system determines in large part the types of risk faced by technology users. These motivations can vary widely, from individuals seeking personal financial gain,[1] to organized criminals offering for-hire botnet infrastructure, to governments seeking to achieve geopolitical goals [7]. Because the computing infrastructure in the developing world presents a set of advantages and disadvantages for cybercriminals, the incentives for attack vary as well.

As a result of these complex relationships, the value of a compromised machine varies between nations. One way to measure the economic value of a compromised machine to cybercriminals is the "pay-per-install" (PPI) price, which is the cost on the global black market to buy rights to install malware per compromised machine. PPI prices for computers in the developing world are significantly (in some cases a full order of magnitude) lower than those in developed world [34]. The market value could be lower for a number of reasons, including greater ease of infection (i.e., increased supply) or lower functionality of developing world hardware (i.e., decreased demand). A better understanding of how compromised machines are used in the developing world would shed light on the forces behind these costs.

Another issue faced in many developing countries is pervasive domestic monitoring, censorship, and other restrictions on the flow of information. While this issue is neither solely a problem of developing nations nor is it ubiquitous among them, freedom of expression is regarded as an important development objective [35]. Improved security techniques and practices, in turn, can help alleviate this problem.

Understanding the motivations behind attacks is a complicated issue, clearly in need of more study. Nevertheless, the perspectives of adversaries must be included to understand the broader security landscape.

3 Challenges for Future Research

Computing security in the developing world is clearly a multifaceted and multidisciplinary problem, and the five factors we identify as defining the security landscape in developing regions offer fertile land for further research. While these represent only a small subset of the issues affecting computing security in the developing world, they highlight several important and pressing challenges in the area.

3.1 Policy

National and international policy plays a major role in influencing security practices, both positively and negatively. Most countries have legacy information and communication technologies (ICT) laws that are inadequate in the face of the rapid and complex changes occurring today, often leading to inadequate or counterproductive policies. For example, India prohibits the use of encryption, a policy justified (ironically) by national security, as it simplifies eavesdropping by authorities. In practice, this exposes its

[1] A common example is the Nigerian letter scam, (also known as "419 fraud").

citizens to attacks by criminals, both domestic and foreign. This policy received significant attention recently, as many major international companies such as RIM, Google, and Skype offer encrypted services in violation of the ban; this is essential to protect their users from identity theft, financial fraud, and other security problems.

3.2 Technical

Several of the unique facets of the security landscape in developing regions call for new technological innovation. The problem of offline infection vectors calls for new virus-protection or virus-cleansing mechanisms which are predominantly designed for the online world. System administrators and kiosk owners need to be better-equipped in handling data loss and corruption that results from sharing PCs across multiple individuals.

The problem of ensuring secure communication on developing-world cellular phone networks is a fascinating research area as well, offering a rich variety of open problems for security researchers. As already pointed out, the mobile phone landscape in developing regions makes it difficult to simply import developed-world solutions for this problem. Given that this landscape is likely to persist for several years [8] and that the demand for security-sensitive applications in developing regions is on the rise, it is a good opportunity for security researchers to do interesting research that can create wide-scale impact. Even the fundamental notions of privacy and authenticity become non-trivial to achieve when operating under these constraints.

Finally, a fundamental problem plaguing the developing world is that of providing digital identities to citizens. In places like India, there is growing emphasis on deploying digital mechanisms to uniquely represent and verify the identity of each individual. It is hoped that such mechanisms will redress some of the problems that disenfranchised citizens have faced in the past due to the inability to uniquely represent themselves in government and other official transactions. Although there are obvious benefits from such systems, if carelessly implemented, these systems could damage individuals' privacy and human rights. Implementing a privacy-preserving unique identity and identification system under developing world constraints like limited infrastructure, intermittent connectivity and poor educational standards, is a problem that requires immediate attention from security researchers[2].

3.3 Business Aspects

Technical procedures and business decisions made by ISPs directly affect subscribers' security. Unfortunately, these decisions are driven by business factors and often pay little concern to user security. For instance, an ISP's decision to deploy ADSL modems that do not support NAT exposes subscribers to malicious incoming connections. A study by Cui et al. [36] identified at least 540,000 publicly accessible embedded devices set with a default password, and their findings suggest that the actual numbers are much higher. Perhaps unsurprisingly, 80% of the vulnerable devices identified were in Asia. Our own observations from India confirm that BSNL, India's largest telecommunications company, also installed ADSL routers that were configured with default passwords, and were not configured to support NAT. What factors drive leading Asian ISPs to make these poor security decisions while their North American and European counterparts choose more wisely? We suspect the sheer volume and fast growth rates of subscribers in Asia play a role, as do considerations about maintenance and support. The length of the purchasing process is likely another factor and is affected by purchasing volumes as well as political and regulatory environments.

3.4 Awareness and Education

Increased awareness of security risks and practices is crucial to improving the computer security situation throughout the developing world, and educating users about these is itself a challenging problem. Affecting this change requires solid grounding in the current state of security education; this present state is largely unknown and unstudied in many developing regions. Indeed, while many of our points about security are based on only anecdotal reports, they suggest potentially significant variations in the way developing world users perceive computing security. In particular, there are many open questions regarding what the actual impact of poor security practices has been on development outcomes. Another related question is how these issues impact organizations such as businesses and governments; indeed, poor computing security practices in these environments can have significant direct and indirect consequences.

4 Conclusion

At its core, the goal of computing security is to ensure users of computing systems can trust and rely upon those systems to accomplish their desired tasks. Failures in computing security present direct impacts, but more fundamentally they undermine the utility of a society's computing infrastructure. Increasing access to, relevance of, and reliance upon ICTs in developing regions promises significant development benefits. While the problems that poor computing security presents to these users may be merely inconveniences today, without the trust and reliability that are provided by strong computing security the promise of ICTs for development will not be fully realized.

We have reached an unusual paradox: most of the people affected by computer security are outside the focus of its research and design, and every year the disparity grows. Although different, the problems of users in developing regions are at least as interesting, and increasingly important – for users, for development, and for overall global security.

Issues such as shared computers, limited training and literacy, and piracy all require a combination of disciplines to achieve real improvements in security. The problems

[2]The UID project in India is attempting to build a biometric-based identification system for citizens which would operate even in locations with poor connectivity. A security analysis of the privacy preserving mechanisms used by this project is missing in the literature.

are only part technical, but nonetheless require both new research and technical leadership to drive policy, education, and the deployment of more secure systems.

5 References

[1] "Norton Cybercrime Report: The Human Impact," 2010.

[2] "M86 security Labs, Spam source by country." "http://www.m86security.com/labs/spam_statistics.asp", 2011.

[3] "Project Honey Pot Statistics." "http://projecthoneypot.org/statistics.php", 2010.

[4] "AirJaldi.Org - Wireless Network, Dharamsala, India." http://www.airjaldi.org.

[5] G. Maier, A. Feldmann, V. Paxson, R. Sommer, and M. Vallentin, "An assessment of overt malicious activity manifest in residential networks," in *DIMVA'11: Proceedings of the Conference on Detection of Intrusions and Malware and Vulnerability Assessment*, Springer, July 2011. to appear.

[6] H. Pal, S. Nedevschi, and Rabin, "A multidisciplinary approach to open access village telecenter initiatives: the case of akshaya," *E-Learning*, vol. 3, pp. 291–316, Sept. 2006.

[7] B. Krebs, ""stuxnet" worm far more sophisticated than previously thought," 2010.

[8] S. Panjwani, "Towards end-to-end security in branchless banking," in *Workshop on Mobile Computing Systems and Applications (HotMobile)*, ACM, Mar. 2011.

[9] F. A. Initiative, "M-Kesho in Kenya: A new step for M-Pesa and mobile banking." http://financialaccess.org/node/2968, May 2010.

[10] "Security breach at m-pesa." http://www.telco2.net/blog/2010/02/security_breach_at_mpesa_telco.html, 2010. Telco 2.0.

[11] S. Panjwani and E. Cutrell, "Usably secure, low-cost authentication for mobile banking," in *Proceedings of the Sixth Symposium on Usable Privacy and Security*, SOUPS '10, (New York, NY, USA), pp. 4:1–4:12, ACM, 2010.

[12] M. Paik, "Stragglers of the herd get eaten: security concerns for gsm mobile banking applications," in *Proceedings of the Eleventh Workshop on Mobile Computing Systems & Applications*, HotMobile '10, (New York, NY, USA), pp. 54–59, ACM, 2010.

[13] E. Brewer, M. Demmer, B. Du, M. Ho, M. Kam, S. Nedevschi, J. Pal, R. Patra, S. Surana, and K. Fall, "The case for technology in developing regions," *IEEE Computer*, vol. 38, no. 6, pp. 25–38, 2005.

[14] R. Cáceres, C. Carter, C. Narayanaswami, and M. Raghunath, "Reincarnating pcs with portable soulpads," in *Proceedings of the 3rd international conference on Mobile systems, applications, and services*, MobiSys '05, (New York, NY, USA), pp. 65–78, ACM, 2005.

[15] A. R. Garuba, "Computer virus phenomena in cybercafé," *Security and Software for Cybercafes*, p. 186, 2008.

[16] O. B. Longe and F. A. Longe, "The nigerian web content: Combating pornography using content filters," *J. Information Tech. Impact*, vol. 5, 2005.

[17] "World Bank, World Development Indicators," 2009.

[18] M. B. Schmidt, A. C. Johnston, K. P. Arnett, J. Q. Chen, and S. Li, "A cross-cultural comparison of us and chinese computer security awareness," *Journal of Global Information Management*, vol. 16, no. 2, p. 91, 2008.

[19] C. C. Zou, D. Towsley, and W. Gong, "Email virus propagation modeling and analysis," *Department of Electrical and Computer Engineering, Univ. Massachusetts, Amherst, Technical Report: TR-CSE-03-04*, 2003.

[20] C. Kanich, C. Kreibich, K. Levchenko, B. Enright, G. M. Voelker, V. Paxson, and S. Savage, "Spamalytics: An empirical analysis of spam marketing conversion," pp. 3–14, 2008.

[21] J. Goodman, G. V. Cormack, and D. Heckerman, "Spam and the ongoing battle for the inbox," *Communications of the ACM*, vol. 50, no. 2, pp. 24–33, 2007.

[22] J. E. Phelps, R. Lewis, L. Mobilio, D. Perry, and N. Raman, "Viral marketing or electronic word-of-mouth advertising: Examining consumer responses and motivations to pass along email," *Journal of Advertising Research*, vol. 44, no. 04, pp. 333–348, 2004.

[23] B. Taylor, "Sender reputation in a large webmail service," 2006.

[24] M. D. Kibby, "Email forwardables: folklore in the age of the internet," *New Media & Society*, vol. 7, no. 6, p. 770, 2005.

[25] M. Sunner, "Developing world, developing problems," *Risk Management & BCDR (MessageLabs)*, no. 9, 2009.

[26] P. Y. K. Chau, M. Cole, A. P. Massey, M. Montoya-Weiss, and R. M. O'Keefe, "Cultural differences in the online behavior of consumers," *Communications of the ACM*, vol. 45, no. 10, pp. 138–143, 2002.

[27] S. Kannan, "Social networking sites prone to virus attacks," *The Hindu*, 2009.

[28] B. Gu and V. Mahajan, "The benefits of piracy - a competitive perspective," 2004. WISE 2004: Workshop on Information Systems and Economics.

[29] T. T. Moores, "An analysis of the impact of economic wealth and national culture on the rise and fall of software piracy rates," *Journal of business ethics*, vol. 81, no. 1, pp. 39–51, 2008.

[30] K. Bagchi, P. Kirs, and R. Cerveny, "Global software piracy: can economic factors alone explain the trend?," *Communications of the ACM*, vol. 49, no. 6, pp. 70–76, 2006.

[31] A. Katz, "A network effects perspective on software piracy," *University of Toronto Law Journal*, vol. 55, no. 2, pp. 155–216, 2005.

[32] P. K. Yu, "Still dissatisfied after all these years: Intellectual property, post-wto china, and the avoidable cycle of futility," *Georgia Journal of International and Comparative Law*, vol. 34, 2005.

[33] J. Karaganis, "Media piracy in emerging economies," 2011. Social Science Research Council.

[34] K. Stevens, "The Underground Economy of the Pay-Per-Install (PPI) Business." Blackhat Conference 2010.

[35] A. Sen, *DEVELOPMENT AS FREEDOM.* Alfred A Knopf, 1999.

[36] A. Cui, Y. Song, P. Prabhu, and S. Stolfo, "Brave new world: Pervasive insecurity of embedded network devices," pp. 378–380, 2009.