Chaperone: a content filtering web proxy based on public health policies

Vasileios Vlachos
Department of Computer Science and Telecommunications
Technological Educational Institute of Larissa
Email: vsvlachos@gmail.com

Vassilios Karakoidas
Department of Management Science and Technology
Athens University of Economics and Business
Email: bkarak@aueb.gr

***Abstract*—In order to contain infectious diseases, public health policies suggest measures to minimise the threats of various risky behaviours. Examples of these measures are the use of condoms for the sexually overactive populations and clean needles for drug addicted users. Computer users that tend to explore various thematic areas (adult sites, warez - pirated software, celebrities and wallpapers) of the World Wide Web have more probabilities to encounter malware problems than others. In this paper we present the CHAPERONE content filtering web proxy, which is able to semantically analyse web sites and automatically adjust its security level accordingly. Sites with questionable, arguable or suspicious content are never blocked but treated differently from the rest of the sites, as they often represent the source of various security infringements.**

I. INTRODUCTION

The problem of malicious software (malware) exists for more than 25 years [1]. The reason that the research community is unable to tackle this problem lies in the evolutionary nature of digital threats. New species of malcode adapt to the developments in Information and Communication Technologies (ICT) so as to survive and use the environment at their benefit. Characteristic examples of these new trends are rapid malcode capable of infecting the susceptible population in less than 10 minutes according to empirical evidence [2] and theoretic *Flash* worms that are able to penetrate most vulnerable systems in less than one minute or according to latest research in few milliseconds [3], [4], [5]. Clearly this approach utilizes upgrades to the global network infrastructure and the corresponding significant increase of the available bandwidth per user via the DSL, cable, satellite or 3G connections. Other forms of malware have found their own role, or niche in the new generation of mobile devices [6], [7], [8] such as cellular devices, smart phones, PDAs etc. The most significant increase of malicious acts has found fertile grounds in the wide adaption of the Internet, both geographically and demographically. As a result the overwhelming majority of users is not aware even for the most fundamentals of computer security [9]. These users are almost exclusively the victims of phishing attacks and other computer related scams [10].

Most importantly, novice or naive home users tend to engage in various activities that are prone to security incidents. These activities include the interaction with web servers with questionable content (pornography, hacking, activism) or the uncontrolled downloading of software. Furthermore, other users try to deliberately obtain software via illegal means (e.g. warez, torrents). Although some of these activities raise various ethical or even legal issues (downloading pirated software), the majority of them are legal in most western countries. On the other hand even a legal activity (e.g. adult pornography), isn't necessarily widely considered a remarkable or at least socially acceptable behavior. Therefore most users would not openly discuss or report possible problems they may encounter in similar websites. The number of adult web-pages (more than 245.000.000 google results for the word "porn") indicates the great interest for similar content. A number of these sites operate on subscription basis, whereas others seem to be free [11]. Recent research confirms that a significant part of these "free"' sites hosts a sufficient number of the general malware activity [12].

Current security applications strive to improve their detection techniques in order to identify and eliminate the new threats resulting in a continuing arms race between malware writers and security researchers, which will not end in the predictable future. The advances in antiviral technology are mostly focused on technical approaches that extend and enhance the two most prominent techniques, namely *signature matching* and *behavioral analysis* [13], [14], [15]. In other words most of the efforts against malcode employ technological means only and treat the cyberspace as a flat environment where all the threats are homogeneously distributed. This paper proposes a personal web proxy which is able to identify risky on line behavior and autonomously adapt hardened security measures. On the other hand during normal browsing activity the browser operates with normal security settings. The system during its operation doesn't require any manual intervention on the user's part, though some optional informative messages about the security status of the browser are available. In Section II we present the related work both in computer security and in other related scientific fields. Section III demonstrates a working prototype and explains its architectural and technical details, while Section IV discusses the benefits and the shortcomings of our methodology. Section IV describes possible additions to our system and concludes this paper.

II. Related Work

The theoretical foundation of our work lies in the area of biosciences and epidemiology. These two scientific fields provide excellent tools and methodologies to understand the reasons that contribute to epidemics in the first place, and most importantly to minimize the effects of infectious diseases - or computer malcode in our context. It should not be overlooked that the earlier forms of malicious software were in general described as "Computer Viruses" [16], [17], "Computer Worms" [18] and "rabbits" [13], a fact that indicates the semantic similarities between biological pathogens and malware. Researchers explored the analogies of computer malcode and various agents of biological diseases [19]. Other efforts utilized biological concepts to contain malware. Some of them are trying to mimic the functionality of the immunological system [20], [21], [22], [23], [24] or the operations of specific cells of the human body [25], [26]. A more general approach is based on the discrimination between health and sickness [27]. Complementarily, other researchers utilized epidemiological models to capture the propagation dynamics of rapid malcode [28], [29], [30], [31], [32]

Closer to our previous [33], [34] and current work are other efforts [35] which are concentrated on public health policies that are in place against major epidemics (Acquired Immune Deficiency Syndrome – AIDS) and propose equivalent public policies for computer malware.

The technological means to achieve the proposed system are mostly content filtering techniques. Though significant work has be done in this area, both in centralized [36] or collaborative filtering systems [37], the main target is to block the access to specific web locations. This is done either for ethical, legal, statutory or compliance reasons. Even though these technologies were put in place strictly for security reasons, they result in a boolean accept/deny decision. Though this might seem reasonable for large enterprises, home users on the other hand do not want to abolish the right to visit any web page they find interesting or entertaining. Therefore we believe that our approach is unique as it is based on public health theory and practise.

III. Design & Implementation

Chaperone is a content filtering web proxy[1]. In Figure 1, a *User* attempts to access a suspicious web site (http://www.malware.net/). Chaperone acts as mediator between the web browser and the actual content of the web site. It scans the downloaded content, passes it through a series of tests and adjusts the security level of the browser accordingly. In this way, the *User* can still access the desired content.

In most cases, mainstream security applications just forbid the user to access the suspicious content. Therefore the users try usually to override these security restrictions, and turn off these facilities, risking even more the security of their system.

Many browsers (such as *Microsoft Internet Explorer*) already have security zoning integrated into their implementation. Chaperone works in accordance with these infrastructures.

[1]http://en.wikipedia.org/wiki/Proxy_server

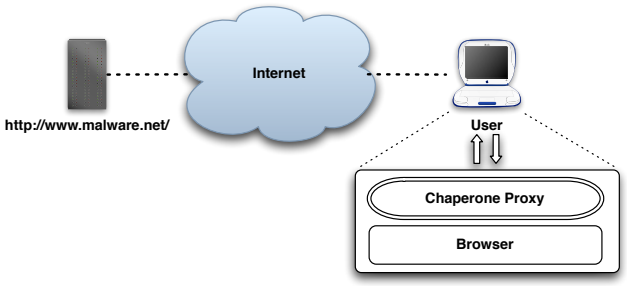

Fig. 1. A Typical Usage Scenario

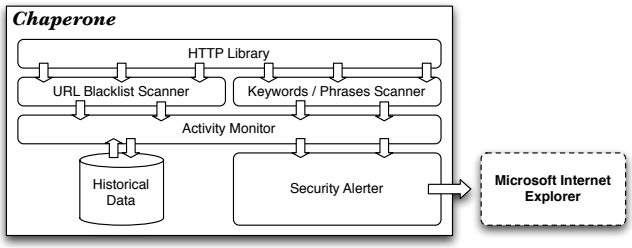

Fig. 2. Chaperone's Architecture

A. Architecture

The architecture of Chaperone is illustrated in Figure 2. The system components are pretty straightforward to understand.

- **HTTP Library** A simple implementation of the HTTP protocol, that downloads the content and forwards it to the scanners.
- **URL Blacklist Scanner** Accepts as input the request's URL and attempts to validate it against Chaperone blacklist.
- **Keyword / Phrases Scanner** In parallel with the *URL Blacklist Scanner* this component scans the content of each HTML page for suspicious keywords.
- **Activity Monitor** This mechanism maintains an archive of browsing history. Both scanners update it and this is the component that actually "decides" the security level of the browser.
- **Security Alerter** The alerter component actually is the only bridge of Chaperone with the outside world. It enforces the browser to raise or lower its security levels and informs the user about potential dangers.

B. Security Mechanisms

Figure 3 is a UML activity diagram that exhibits all the phases of content scanning. These phases are: *(1) URL scan*, *(2) Content Scan*, and *(3) Screening*.

Upon request, *chaperone* downloads the desired content and perform a *URL* and *Content* scan. *URL* scanning includes

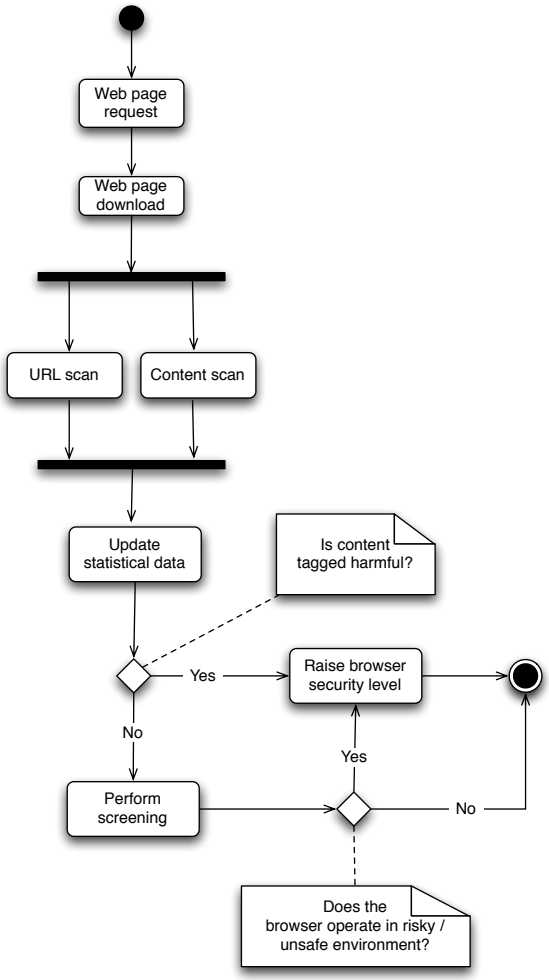

Fig. 3. Content Scanning Algorithm

searching of the web address of the remote address site against a series of blacklisted URLs. *Content* scan analyses semantically the HTML code, and searches for specific keywords that may characterize the page as dangerous for the security of the system. In addition, CHAPERONE checks the MIME types of the content and validates them against the actual files, thus eliminating imposing threats masked as images etc.

When the scanning phase is complete, the system updates its historical database. If the content is tagged as suspicious, CHAPERONE raises the browser's security level. Practically if the security is raised to the highest level, ActiveX controls are disabled, javascript execution is prevented and downloading of content becomes more selective.

Even if the content is safe, the system checks its historical data, and decides whether the system must operate in high security level due to past activity regardless of the current situation. The security levels will drop down to normal when the user invokes a full system scan for malware in their system with the traditional security mechanisms, such as antiviruses etc.

C. Practical Experience

The prototype implementation of CHAPERONE is a native python program. Actually it is a modified version of the publicly available *munchy* HTTP proxy[2]. Our implementation does not support the SOCKS protocol.

The list of the blacklisted URLs was obtained through *Blacklist.com*[3] and the phrases that we used for the keyword search in the HTML code were downloaded from http://contentfilter.futuragts.com/phraselists/.

The current CHAPERONE implementation works only with *Internet Explorer* on *Windows*, since it provides the ability to alter the security settings easily through the windows registry. We suggest to remove the anti-phising mechanism that the *Internet Explorer* provides as a standard feature with version 7 and above. It corrupts the historical data of the of CHAPERONE, since it makes HTTP requests to servers at *Microsoft* to check if the URL is blacklisted and the system is unable to distinguish calls between the security feature and the actual user requests.

IV. DISCUSSION

Recent [38], [39] research confirms that the adversaries that would create a phony site and upload desirable content to it, have probably other intentions than to simply wreak havoc. The more lucrative activities of cybercriminals such as spamming, phishing, extortions, illegal content and counterfeit software require a sufficient number of remotely controlled systems, also known as *zombies* or *bots* to store and host this content and serve their potential customers as well as finding new victims to infect. Recent analysis [40] of modern botnets reveals that malware writers embed highly advanced techniques so as to avoid detection and in most cases to fight back possible efforts to intercept or block the communications of the botnet. The means to perform all these activities are obviously the personal computers of unaware users which also offer the important advantage that makes the identification and prosecution even more difficult. Thus we observe that this situation leads to a vicious cycle. An increased number of initially infected systems would accelerate the overall progress of the infection.

Practical epidemiologists seek measures that are helpful to contain possible epidemics [41]. To succeed in that, they have to accept that public health outweighs possible ethical or even legal questions that may arise because of the behavior of specific individuals or particular groups [42]. Therefore drug addicts constantly get free syringes and needles in order to avoid possible blood-transferred infections such as AIDS or Hepatitis B and C, despite the fact that their drug addiction exposes them to great danger and is illegal in some countries. The rationale behind this counterintuitive practise lies in the the fact it is not reasonable to expect that they will stop obtaining drugs, because of the legal or moral consequences of their acts. On the contrary, they will continue to pursue at

[2]http://arctrix.com/nas/python/munchy.py
[3]http://www.blacklist.com/

any cost their next dose. As a result they may soon became carriers of dangerous contagious diseases if they don't get assistance to perform their activities in a safer way [43]. Another characteristic example is prostitution [42]. Though the percentage of HIV-infected women that participate in that activity is in most western countries small, because of additional proactive measures (e.g. screening [44]), in the developing countries the distribution of condoms in red light districts proved effective to decrease the rate of new HIV infections [42]. The above-mentioned facts indicate the importance to take some protective measures in risky environments.

The outcome of most recent medical studies confirms that is much easier and more useful to convince people to modify or slightly change their habits in order to be more safe than to quit them and completely change their way of life [45]. We start our work based on that particular assumption, and argue that in order to maximize the effects of a computer public health policy, the main effort should be given to computer users. Empirical evidence [46] suggests that arguments against certain activities that we described earlier would not change the behavior of most users. Even strict measures that have been put in practise in some countries [47], which among other include jail sentences and high finess, did not eliminate the traffic towards websites with questionable content. These conditions force users to operate under a secrecy mode in which it is highly improbable they would seek advise if they encountered any problem. Even worse, if they use a non personal system (work or family computer), they will try to conceal their activity, which makes more difficult the timely identification of a possible malware infection.

Current protection methodologies treat the whole World Wide Web (WWW) as a flat area and therefore have a constant security policy. This leads us to the following problem: the default security policy could be sufficient for most web sites, but it may be either too strict for specific web based applications (e-banking) or too relaxed for maliciously crafted malware serving websites. As a result users that repeatedly visit websites with arguable content that operate more or less in a gray area have an increased probability of acquiring an infection compared the rest. If a sufficient number of these systems became infected, they would act as the carrier to bring malware to many other users. In Epidemiology it is well known that the number of the initially infected hosts is a decisive factor regarding the appearance of an epidemic [48], and that holds for Computer Epidemiology as well [3], [5], [28]. It is therefore in the public's best interest to keep the number of infected users as low as possible, even if some of them decided to demonstrate risky online behavior, which includes also popular sites with socially accepted content (wallpapers, screensavers, celebrities) that may host malware. For that reason, as well as because of previous research on the demographics of malware [12], we decided to automatically increase the security level in these and other malware-rich areas, in order to protect most non technical users.

V. Availability

We believe that our work is not as restrictive as the rigid enforcement of blacklisting rules in which the user is prohibited to visit numerous web pages. On the contrary he or she has to accept a minimal loss of functionality only during the interaction with web sites with content that is generally considered to be attracting malware. The Chaperone proxy has been tested in various circumstances with no obvious problems and can work adequately with all recent versions of Internet Explorer (IE 6, IE 7 and IE 8) in modern Microsoft's operating systems (XP and Vista). On the other hand the subject of our research is rather sensitive. We reasonably didn't explore the route of asking volunteers to provide us with data of web activity in adult sites or in pirated software areas. Instead we decided to make available this software under the GPL licence and let any interested party evaluate it. Finally we felt obliged to clarify that our system purposely doesn't provide any protection for web pages that might contain child pornography as it is beyond any logical doubt one of the gravest crimes in the civilized world and therefore the perpetrators should be denied any possible technical assistance nor we want to intervene with any law enforcement activities that target paedophiles.

VI. Concluding Remarks and Future Work

Most users are not willing to accept any limitation or restriction in their web surfing habits and therefore will actively seek to bypass any possible protective measure. We argue that we are able, with the users' consensus, to turn a restrictive technology as blacklisting in to a protective framework by utilizing content filtering techniques. The use of widely available blacklists could identify probable malware hot spots. We are aware that numerous content filtering technologies are much more effective than our simplistic URL filtering and regular - expression pattern matching rules and we are planning to use them in the near future. On the other hand we believe that our effort to adapt long established public health techniques in computer security is a step towards more resilient systems in the face of evolving malware threats.

References

[1] F. Cohen, "Computer viruses: Theory and experiments," in *Proceedings of the 7th national security conference*, September 1984, pp. 240–263.

[2] D. Moore, V. Paxson, S. Savage, C. Shannon, S. Staniford, and N. Weaver, "Inside the slammer worm," *IEEE Security & Privacy*, pp. 33–39, July 2003.

[3] S. Staniford, V. Paxson, and N. Weaver, "How to 0wn the internet in your spare time," in *Proceedings of the 11th USENIX Security Symposium*, August 2002, pp. 149–167. [Online]. Available: http://www.icir.org/vern/papers/cdc-usenix-sec02/

[4] S. Staniford, D. Moore, V. Paxson, and N. Weaver, "The top speed of flash worms," in *WORM '04: Proceedings of the 2004 ACM workshop on Rapid malcode*. New York, NY, USA: ACM Press, 2004, pp. 33–42.

[5] N. Weaver, V. Paxson, and S. Staniford, "A worst-case worm," in *Proceedings of the Third Annual Workshop on Economics and Information Security (WEIS04)*, May 2004.

[6] M. Hyoenen, "Wap and viruses-can your mobile get infected?" in *Proccedings of Virus Bulletin Conference*, September 2000, pp. 39–44.

[7] N. Leavitt, "Mobile phones: The next frontier for hackers?" *IEEE Computer*, vol. 38, no. 4, pp. 20–23, April 2005.

[8] L. Paulson, "First smart-phone virus is discovered," *IEEE Computer*, vol. 37, no. 8, p. 29, August 2004.

[9] M. Boeckeler, "Overview of security issues facing computer users," SANS Istitute, GSEC Practicum v1.4b Option, March 2004.

[10] D. Mosley, "Some psychological factors of successful phishing," Infosocwriters.

[11] B. Edelman, "Red light states: Who buys online adult entertainment?" *Journal of Economic Perspectives*, vol. 23, no. 1, pp. 209–220, 2009.

[12] E. Moshchuk, T. Bragin, S. Gribble, and H. Levy, "A crawler-based study of spyware on the web," 2006.

[13] P. Szor, *The Art of Computer Virus Research and Defense*. Upper Saddle River, NJ: Addison-Wesley, February 2005.

[14] M. Erbschloe, *Trojans, worms and spyware. A computer security professional's guide to malicious code*. Oxford, UK: Elsevier Butterworth–Heineman, 2005.

[15] E. Skoudis, *Malware, Fighting Malicious Code*, 6th ed., ser. Computer Networking and Distributed Systems. NJ, USA: Prentice Hall, 2004.

[16] F. Cohen, "Computer viruses – theory and experiments," *Computers and Security*, vol. 6, pp. 22–35, 1987.

[17] ——, *A Short Course on Computer Viruses*, ser. Wiley Professional Computing. Canada: Wiley, 1994.

[18] J. Shoch and J. Hupp, "The "worm" programs–early experience with a distributed computation," *Computing Practices*, vol. 25, no. 3, pp. 172–180.

[19] J. Li and P. Knickerbocker, "Functional similarities between computer worms and bilogical pathogens," *Computers & Security*, vol. 26, pp. 338–347, 2007.

[20] S. Forrest, S. Hofmeyr, and A. Somayaji, "Computer immunology," *Communications of the ACM*, vol. 40, no. 10, pp. 88–96, 1997. [Online]. Available: citeseer.nj.nec.com/forrest96computer.html

[21] S. Forrest, A. Somayaji, and D. Ackley, "Building diverse computer systems," in *IEEE 6th Workshop on Hot Topics in Operating Systems,*, 1997.

[22] A. Somayaji, S. Hofmeyr, and S. Forrest, "Principles of a computer immune system," in *Meeting on New Security Paradigms, 23-26 Sept. 1997, Langdale, UK*. New York, NY, USA : ACM, 1998, 1997, pp. 75–82. [Online]. Available: citeseer.nj.nec.com/11313.html

[23] A. Somayaji and S. Forrest, "Automated response using system-call delay," in *Nith USENIX security symposium*, 2000.

[24] T. Okamoto and Y. Ishida, "A distributed approach against computer viruses inspired by the immune system," *IEICE Transaction on Communications*, vol. E83-B, pp. 908–915, May 2000.

[25] U. Aickelin and J. Greensmith, "Sensing danger: Innate immunology for intrusion detection," *Information Security Technical Report*, vol. 12, pp. 218–227, 2007.

[26] DangerProject, "The danger project," Current on-line (September 2008): http://http://www.dangertheory.com/, September 2008.

[27] M. Burgess, "Biology, immunology and information security," *Information Security Technical Reports*, vol. 12, pp. 192–199, 2007.

[28] J. Kephart, D. Chess, and S. White, "Computers and epidemiology," *IEEE Spectrum*, vol. 30, no. 20, May 1993.

[29] R. Pastor-Satorras and A. Vespignani, "Epidemic spreading in scale-free networks," *Physical Review Letters*, vol. 86, pp. 3200–3203, 2001. [Online]. Available: citeseer.nj.nec.com/407844.html

[30] J. Leveille, "Epidemic spreading in technological networks," HPL-2002-287, School of Cognitive and Computing Sciences, University of Sussex at Brighton, Bristol, October 2002.

[31] J. Kephart, "How topology affects population dynamics," in *Proceedings of Artificial Life 3*, New Mexico,USA, June 1992.

[32] D. Moore, C. Shannon, G. Voelker, and S. Savage, "Internet quarantine:requirements for containing self-propagating code," in *Proceedings of 22nd Annual Joint Conference of IEEE Computer and Communication Societies (INFOCOM 2003)*, April 2003.

[33] V. Vlachos, A. Raptis, and D. Spinellis, "PROMISing steps towards computer hygiene," in *International Network Conference (INC2006)*, S. Furnel, Ed., Plymouth, UK, July 2006, pp. 229–236.

[34] V. Vlachos and D. Spinellis, "A PRoactive malware identification system based on the computer hygiene principles," *Information Management and Computer Security*, vol. 15, no. 4, pp. 295–312, 2007. [Online]. Available: http://www.dmst.aueb.gr/dds/pubs/jrnl/2007-IMCS-Promise/html/VS07.html

[35] K. Zelonis, "Avoiding the cyber pandemic: A public health approach to preventing malware propagation," Master's thesis, Carnegie Mellon University, December 2004.

[36] C. Ding, C. Chi-Hung, J. Deng, and D. Chun-Lei, "Centralized content-based web filtering and blocking: How far can it go?" in *IEEE INTERNATIONAL CONFERENCE ON SYSTEMS MAN AND CYBERNETICS*, 1999, pp. 115–119.

[37] J. B. Schafer, D. Frankowski, and J. Herlocker, "Collaborative filtering recommender systems," *Lecture Notes in Computer Science*, no. 4321, pp. 291–324, 2007.

[38] T. Holz, "A short visit to the bot zoo," *IEEE Security & Privacy*, vol. 3, no. 3, pp. 76–79, May 2005.

[39] D. Geer, "Malicious bots threaten network security," *IEEE Computer*, vol. 38, no. 1, pp. 18–20, January 2005.

[40] P. Barford and V.Yegneswaran, "A look inside botnets," in *In Series: Advances in Information Security*, Springer, Ed., February 2007, pp. 171–191.

[41] D. Trichopoulos, *Epidemiology, principles, methods*. Athens, Greece: Scientific Publications Gr. Parisianos, 1982, (Text in Greek).

[42] A. Singhal and E. Rogers, *Combating AIDS: Communication Strategies in Action*. California, USA: Sage Publications, 2003.

[43] J. Watters, M. Estilo, G. Clark, and J. Lorvick, "Syringe and needle exchange as hiv/aids prevention for injection drug users," *Journal of American Medical Association*, vol. 271, no. 2, pp. 115–120, January 1994.

[44] G. Sanders, A. Bayoumi, V. Sundaram, S. Bilir, C. Neukermans, C. Rydzak, L. Douglass, L. Lazzeroni, M. Holodniy, and D. Owens, "Cost-effectiveness of screening for HIV in the era of highly active antiretroviral therapy," *The New England Journal of Medicine*, vol. 352, no. 6, pp. 570–585, February 2005.

[45] S. Krippax and K. Race, "Sustaining safe practice: Twenty years on," *Social Science & Medicine*, vol. 57, no. 1, pp. 1–12, 2003.

[46] A. Adams and M. Sasse, "Users are not the enemy," *Communications of the ACM*, vol. 42, no. 12, pp. 41–46, December 1999.

[47] J. Lu and I. Weber, "State, power and mobile communication: a case state, power and mobile communication: a case study of china," *New Media & Society*, vol. 9, no. 6, pp. 925–955, 2007.

[48] D. Daley and J. Gani, *Epidemic Modelling*. Cambridge, UK: Cambridge University Press, 1999.