Usability Analysis of Sophos Antivirus

Jacky Cheung, Stanley Li, Alex Totolici, Patrick Zheng, *EECE 412*
jackycheung478@hotmail.com, lehaihua444@msn.com, alex.totolici@gmail.com,
patrickzheng1987@hotmail.com

***Abstract*— This paper highlights some of the positive and negative aspects of Sophos Antivirus, in an effort to rate its usability. A user survey, cognitive walkthrough and heuristic evaluation were performed in order to collect appropriate information and identify problem areas. The survey provides a statistical representation of how first-time users feel about the usability of Sophos Antivirus compared to other security software. The cognitive walkthrough highlights the ways in which Sophos helps or hinders users' tasks by looking at a few common task scenarios. The heuristic evaluation brings to light the flaws identified in Sophos' interface, and assigns a level of severity to each, considering the impact that these issues have on users. A brief comparison with other antivirus software is made, to understand how other providers deal with usability in their applications.**

***Index Terms*—Sophos, antivirus, HCIsec, usability**

I. Introduction

ANTIVIRUS software is a necessity of modern computing, as it provides users with protection against malware of many kinds. The highly networked nature of computing leaves end-users at risk from viruses, Trojan horses, spyware, adware, and worms, and antivirus software (AVS) is what many turn to for protection. There are many different options for users looking to purchase an AVS on the market, including Norton Antivirus, Norman, McAfee and Sophos. Different offerings have different feature sets as well as different levels of usability. Users will choose to purchase a certain AVS less because of the intricate technical details, and more because of the software's ease of use. If security software is hard to manage by end-users, it loses its effectiveness. In the case of antiviral software, where the majority of the user-base is not comprised of computer-savvy users, usability issues may prompt users to altogether disable the software, or make poor decisions, thus leaving the user insecure and unprotected.

This paper focuses on the analysis of Sophos' antivirus, version 7.6.1. Sophos is widely used in many universities including Aberdeen[2], University of Liverpool[3] and the University of British Columbia[4]. Students and staff are able to download and install this software free of charge. As the University is endorsing the software, users may place an implicit trust and accept it as one of the better offerings in terms of AVS. Users that find the software unusable may become frustrated, either ignoring its errors or completely disabling it. As a commercial product, Sophos must maintain a good and easy-to-use user interface (UI) in order to provide for its customers a comfortable mechanism for dealing with malware, all the while considering that many of those that require antivirus software are not computer literate.

This report is divided as follows: section II covers some of the related work done in the field. Section III gives an overview of the cognitive walkthrough performed on Sophos, and Section IV continues with the heuristic evaluation. Section V analyzes the psychological impact of usability and summarizes our user survey. Section VI gives a comparison between Sophos antivirus and two alternatives: Norton Antivirus 2009 and Norman, and how usability affects their customer base. Section VII summarizes the findings, and Section VIII concludes with an overall account of the usability of Sophos and suggestions for future improvements.

II. Related Work

Human-Computer Interaction (HCI) is the main academic area dealing with usability of user interfaces. The Cognitive Walkthrough and the Heuristic Evaluation[1] are established methods that HCI professionals use to rate the usability and ease-of-use of interfaces.

Most of the analyses concerning antivirus software focus on the relative technical ability of the product under review to detect, quarantine or clean infections. We feel that focusing on just technical merits in order to rate antivirus software is ignorant of the real-world requirements of users, and that more usability studies are required in this area.

Manuscript received October 9, 2001. (Write the date on which you submitted your paper for review.) This work was supported in part by the U.S. Department of Commerce under Grant BS123456 (sponsor and financial support acknowledgment goes here). Paper titles should be written in uppercase and lowercase letters, not all uppercase. Avoid writing long formulas with subscripts in the title; short formulas that identify the elements are fine (e.g., "Nd–Fe–B"). Do not write "(Invited)" in the title. Full names of authors are preferred in the author field, but are not required. Put a space between authors' initials.

F. A. Author is with the National Institute of Standards and Technology, Boulder, CO 80305 USA (corresponding author to provide phone: 303-555-5555; fax: 303-555-5555; e-mail: author@ boulder.nist.gov).

S. B. Author, Jr., was with Rice University, Houston, TX 77005 USA. He is now with the Department of Physics, Colorado State University, Fort Collins, CO 80523 USA (e-mail: author@lamar.colostate.edu).

T. C. Author is with the Electrical Engineering Department, University of Colorado, Boulder, CO 80309 USA, on leave from the National Research Institute for Metals, Tsukuba, Japan (e-mail: author@nrim.go.jp).

III. Cognitive Walkthrough

The first stage in our assessment of Sophos' usability was to perform a cognitive walkthrough, looking at the most common tasks average users will perform. For that, we have selected:

1. Installation of Sophos Antivirus
2. Running the initial, full system scan
3. Scheduling automated scans
4. Dealing with a virus infection

A. *Installing Sophos*

The installation of Sophos is a two stage process: users first retrieve a download helper application from their respective University's IT department website, and then allow this tool to download and install the actual setup executable. No cognitive issues have been identified at this step.

B. *Full system scan*

Running the initial, full system scan is not difficult, since the software's main application window has a button clearly labeled for that task.

C. *Automated Scans*

When users want to schedule a scan for their computer, they first need to open up the application and then choose "set up a new scan". Then, users should click "Schedule this scan" at the bottom of the view to configure the schedule. However, this function is actually accessed via a hyperlink, and users that may be looking for a button will overlook it. Users may altogether assume that Sophos does not allow for scheduled scans. Once users reach the scheduling view, they are able to configure the scan. For example, if a user wants to set up a scan for every weeknight at 3 a.m., then the user should put the put check mark for initial the plan first. Secondly, the user should put check mark on Monday, Tuesday, Wednesday, Thursday, and Friday. Thirdly, the user should add the time "3:00". Finally, the user should enter the username and password of an administrator account. If a user also wants to set up a scan for every weekend night at 5 am, then the user would need to set up another scan.

D. *Dealing with a Virus*

When a virus is identified, Sophos will display a popup alert above the users taskbar (Fig. 1). This popup, however, does not allow the user to act upon the virus, and no further information is given on how the user should proceed. First-time users may either panic—in which case they will probably open the Sophos interface to use the help functionality—or incorrectly assume that the problem has been resolved automatically. This has the potential of leaving systems vulnerable and unusable: Sophos blocks access to infected files.

Fig. 1 Popup window shown when a virus is detected

IV. Heuristic Evaluation

The heuristic evaluation performed, using Jakob Nielsen's 10 heuristic principles[1], has been conducted at the same time as the cognitive walkthrough.

- The most egregious issue with Sophos' interface is the inconsistency present all throughout. Buttons are represented either as normal Windows buttons or as hyperlinks, many in different styles. There is no transfer effect for users from the rest of the operating system, and a high degree of confusion may stem from a user's uncertainty about what a certain link does.
- The help system is awkward and unintuitive: when a user brings up the help interface, they are taken to the default help view, instead of a more intelligent, context-based one. A user that decided to access help from the Quarantine view is almost certainly interested in dealing with quarantined items, less so with system scans, and the Sophos help system should aid users reach the information they need as quickly as possible.
- When requiring the user to enter an administrator account's details, for a scheduled scan, Sophos will not inform the user as to why this information is required. An error message is presented if the user forgets to type a password (or if they type an incorrect one), but this message is full of jargon.
- Bringing up the main Sophos application window is in violation of the standards commonly accepted by applications on the Windows platform. Sophos resides in the systray, as it runs in the background. While most applications that have the same behaviour open in response to a double-click on their corresponding systray icon, Sophos will begin its update process. Users must right-click and identify the correct option in the menu before they

can open the interface (Fig. 2)

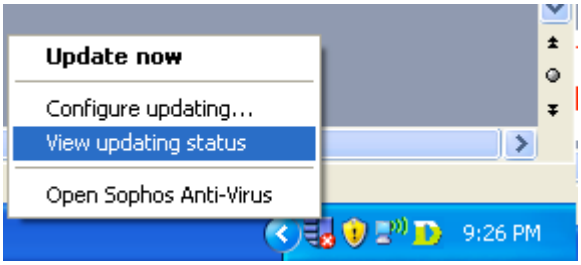

Fig. 2 - Users have to right-click on the Sophos systray icon before they can open the application.

V. Psychological Impact

Psychological impact plays a significant role in how users evaluate the efficiency and usability of software. By definition, psychological impact includes the use of pop-up, animation, efficient use of wordings and color to attract users' attentions so that users can be notified about security warnings in an efficient manner, one that is also effective at communicating to users the urgency and nature of their required interaction.

Sophos guides users step-by-step during its installation phase by constantly providing feedback as to what the current action is. Buttons are used to highlight the actions and options available. This design is efficient in communicating to users what the next action is, even though they may not understand what is going on behind the scenes. The button labels are clearly marked so as to avoid errors on the part of the user, and installation is automated and painless.

In terms of notifying users about virus infection, Sophos uses jargon that alienates average computer users, and a popup that does not help users in understanding what is required of them in the next step. Once users open the main application window, they still need to identify that the Quarantine is where viruses are stored, until further action is taken. The link that takes users to the Quarantine window is not very visible, however once on that view, things become easy. Options and available actions are clearly listed and self-explanatory, allowing users to complete their task. In terms of psychology, deleting a virus is really simple, a single button click. This design really motivates users to click and delete the infected files, which in certain cases may not be the best solution. However, in terms of keeping the system secure, Sophos does help users clean problematic files easily.

Performing a virus scan is not intuitive. Except for the full system scan, multiple steps are needed before a user's goal will be reachable, as shown in the cognitive walkthrough for setting up a scheduled scan.

A survey was conducted on a sample of 30 users, attempting to understand the level of comfort they have experienced in dealing with Sophos AV (Appendix A).

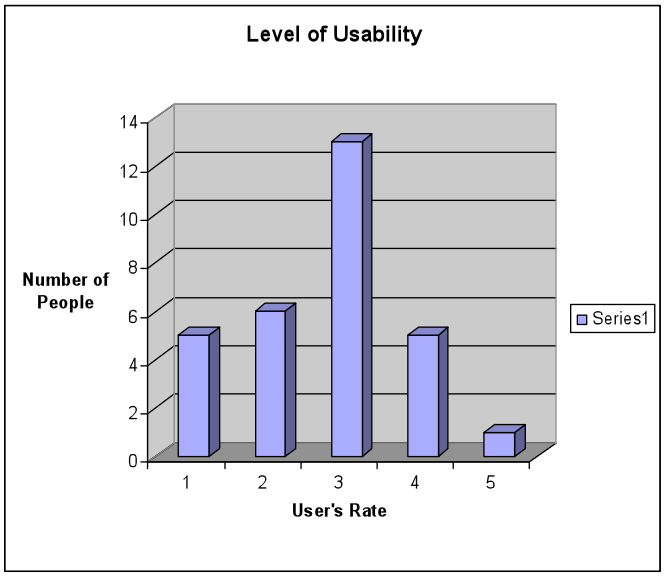

Fig. 3 – Likert-scale results for users' overall rating of the usability of Sophos AV

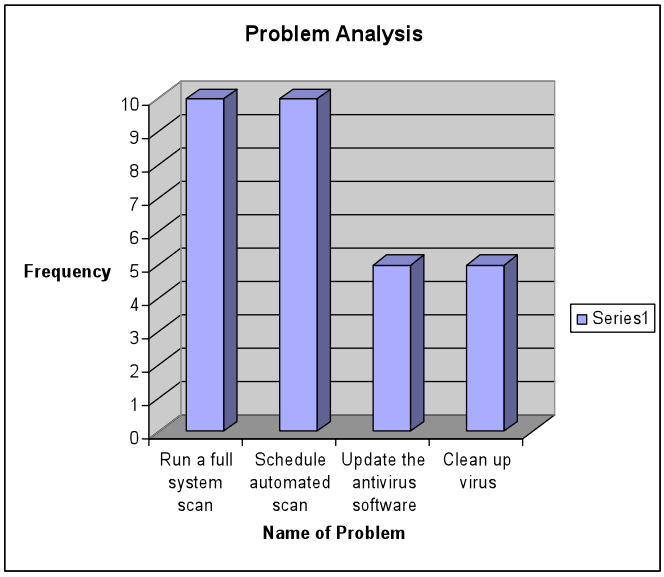

Fig. 4 – Tasks that users found to be difficult to perform

A discussion of the results is provided in Section VII.

VI. Comparisons with Norton AV and Norman VC

A brief comparison was made between Sophos, Norton Antivirus and Norman Virus Control, in order to understand how other vendors handle usability problems and learn how Sophos may improve.

A. Norton AV

Norton's installation procedure is similar to Sophos', however more information is presented to users regarding the actions that are performed in the background. While this information may be useful to some, we consider that average users are not interested in technical details, as long as things are working.

The update process in Sophos is very subtle, and does not interfere with the user in any way. However, it is almost invisible, and when updates are not found, no kind of message is displayed. Norton has a very visible update mechanism, which, while not falling into the trap of over-informing users about what is going on, may be clearer.

Scheduling scans is easier in Norton, as users can set different schedules for one scan, and more importantly can set-up scans upon computer startup, user login, or when the system is idle. More freedom makes Norton a more usable alternative in this regard.

Norton automatically deletes infected files, while still informing users via a popup. The systems are similar in this regard.

B. *Norman VC*

Norman does not automatically update its virus definitions upon install. This leads to a false sense of security, as without the most recent virus signatures, users are not really protected.

Norman is over-engineered in terms of scan options. While Sophos has power-user options available via its menus, the initial interface is not overly complex. Norman readily confuses users due to the various scan options available.

VII. Discussion

The problems discovered during the cognitive walkthrough and the heuristic evaluation highlight the need for a revisiting of Sophos' interface by the software's designers. Except for the virus alert popup issue, none of the identified problems are showstoppers on their own. However, they never surface independently, either. The most important aspect to consider, in evaluating the overall usability of Sophos, is the likelihood that users will make a poor decision as a result of any of the identified issues. As stated, the lack of control on the popup alert is the most likely point where users will make a mistake. The lack of information about how users must continue may lead many to assume that no action is required on their part, and while the virus will not continue spreading on the local system at that point, many applications will be blocked by Sophos. Users need to be made aware that they need to clear the virus threat and then reinstall some of the affected executables.

Although most survey users rated the overall usability of Sophos with a 3 out of 5, we can see in Fig. 3 that the 'average' is below 3. Most problematic areas, as reflected in Fig. 4, were the scan modes, whereby we may conclude that most users are happy if the antivirus does everything for them in the background.

Our suggestions revolve around ensuring that users are made clear on the urgency of the interaction that is required of them. More specifically, taking advantage of transfer effects (by making the Sophos interface as similar to standard Windows interfaces as possible) and effective metaphors (i.e. a red stop sign when a user's action is required to proceed) are the easiest fixes to implement, and ones that would address most of the issues discovered.

VIII. Conclusion

Sophos antivirus is not a completely unusable piece of software, though it does not shine in any particular way. Students and staff may keep using it because their University provides it free of charge, but other alternatives, superior in terms of usability, are available. Sophos may leave end-user's system vulnerable as a result of some of the interface problems, and it is therefore suggested that as many of these problems are addressed by the makers of Sophos.

Appendix A – Survey Questions

A. *General*

1. What antivirus are you currently using?
    a. Norton Antivirus
    b. Sophos Antivirus
    c. McAfee
    d. AVG
    e. Microsoft OneCare
    f. Kaspersky Antivirus
    g. Norman Antivirus
    h. AVIRA
    i. GDATA
    j. Other _____
2. What major tasks do you usually perform using your antivirus?
    a. Run a full system scan
    b. Schedule an automated scan
    c. Update the antivirus software
    d. Clean up virus
    e. Others_____

B. *After using Sophos*

1. When performing all your major tasks using Sophos, please indicate the level of complexity
    a. Easy
    b. Medium
    c. Hard
2. Are you able to get help if you needed?
    a. Yes
    b. No
    c. No help is needed
3. Please rate the usability level of Sophos (1 to 5)
4. Compared to your own antivirus, which one do you prefer?
    a. Sophos
    b. Your own antivirus_____
5. Where do you think Sophos is most effective?
    a. Run a full system scan

   b. Schedule an automated scan
   c. Update the antivirus software
   d. Clean up va irus
6. Where do you think Sophos is most effective?
   a. Run a full system scan
   b. Schedule an automated scan
   c. Update the antivirus software
   d. Clean up a virus

REFERENCES

[1] [1] J. Nielsen, "Ten Usability Heuristics," 2005. [Online]. Available: http://www.useit.com/papers/heuristic/heuristic_list.html. [Accessed: Nov.30, 2008].

[2] University of Aberdeen, "Sophos :: Anti-Virus software," Nov. 19, 2007. [Online]. Available: http://www.abdn.ac.uk/dit/antivirus/. [Accessed: Nov.30, 2008].

[3] University of Liverpool, "Sophos Anti-Virus Software for home use or MWS machines," 2004. [Online]. Available: http://antivirus.liv.ac.uk/. [Accessed: Nov.30, 2008].

[4] University of British Columbia, "UBC IT's Software Downloads," Oct.1, 2008. [Online]. Available: **http://www.it.ubc.ca/download.html**. [Accessed: Nov.30, 2008]