UNDERSTANDING THE USER CAN BE A TOOL FOR CYBER DEFENSE

Gina F. Thomas, Samuel R. Kuper, Krystal M. Thomas, Erik W. Armbrust, and Michael W. Haas
Air Force Research Laboratory
March 2012

Distribution A: Approved for public release; distribution unlimited.
Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th Air Base Wing Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RH-WP-TP-2012-0031 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

\signed\GINA F. THOMAS
Work Unit Manager
Collaborative Interface Branch
Warfighter Interface Division

\signed\WILLIAM E. RUSSELL
Chief, Collaborative Interface Branch
Warfighter Interface Division

\signed\MICHAEL STROPKI
Chief, Warfighter Interface Division
Human Effectiveness Directorate
711Human Performance Wing

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government’s approval or disapproval of its ideas or findings.
4. TITLE AND SUBTITLE
UNDERSTANDING THE USER CAN BE A TOOL FOR CYBER DEFENSE

6. AUTHOR(S)
Gina F. Thomas, Samuel R. Kuper, Krystal M. Thomas, Erik W. Armbrust, and Michael W. Haas

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Applied Neuroscience Branch
Wright-Patterson Air Force Base, OH 45433

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Materiel Command
Air Force Research Laboratory
711 Human Performance Wing
Human Effectiveness Directorate
Warfighter Interface Division
Applied Neuroscience Branch
Wright-Patterson Air Force Base, OH 45433

12. DISTRIBUTION/AVAILABILITY STATEMENT
Distribution A: Approved for public release; distribution unlimited.

13. SUPPLEMENTARY NOTES
88 ABW Cleared 04/02/2012; 88ABW-2012-1900. Report contains color.

14. ABSTRACT
There is little question that Cyber Defense Analysis is a complex and difficult activity. The shear immensity of cyberspace and the inconsistency of attacks requires a comparable effort in terms of aiding. This paper suggests that an understanding of end user experiences and behaviors could be utilized to provide information and support to analysts. In order to attain that understanding, we propose that, in addition to and in support of the development of new technologies and tools, research is needed that focuses on understanding the interactions between cyber attack, end users’ psychological states, behavioral indicators of those states and individual characteristics that are likely to mediate behavioral responses.

15. SUBJECT TERMS
cyber defense, personality, psychological state, affect, emotion

16. SECURITY CLASSIFICATION OF:
a. REPORT Unclassified
b. ABSTRACT Unclassified
c. THIS PAGE Unclassified

17. LIMITATION OF ABSTRACT: SAR

18. NUMBER OF PAGES 7

19a. NAME OF RESPONSIBLE PERSON (Monitor)
Gina F. Thomas

19b. TELEPHONE NUMBER (Include Area Code)
Understanding the user can be a tool for cyber defense.


1,2,3,4,5 Air Force Research Laboratory, 711 Human Performance Wing, 2510 5th Street, Wright Patterson AFB, OH 45433

Abstract

There is little question that Cyber Defense Analysis is a complex and difficult activity. The sheer immensity of cyberspace and the inconsistency of attacks requires a comparable effort in terms of aiding. This paper suggests that an understanding of end user experiences and behaviors could be utilized to provide information and support to analysts. In order to attain that understanding, we propose that, in addition to and in support of the development of new technologies and tools, research is needed that focuses on understanding the interactions between cyber attack, end users’ psychological states, behavioral indicators of those states and individual characteristics that are likely to mediate behavioral responses.

Keywords: cyber defense, personality, psychological state, affect, emotion.

1 Corresponding author. Email: gina.thomas@wpafb.af.mil

1. Introduction

According to the National Security Strategy, “Cybersecurity threats represent one of the most serious national security, public safety, and economic challenges we face as a nation” (2010). In addition to widespread dependence on networking in the private sector, the Department of Defense relies on the cyberspace domain to conduct multiple operations worldwide. Increasing dependence brings about increasing vulnerability. The Department of Defense (DoD) has publicly recognized the inadequacy of cybersecurity and has set policy to increase it as a national priority (DoD, 2011).

Cyberspace is an enormous domain. There are “over 15,000 networks and seven million computing devices across hundreds of installations in dozens of countries around the globe” operated by the DoD alone and over 2 billion independent users of the internet (DoD, 2011). Yet a very small percentage (less than 0.1%) of our military conducts or supports cyber defense. Cyber Defense Analysts are expected to detect, report, and mitigate damages from intrusions in a domain that does not occupy space in the same way as other domains. Their task requires vigilance intermittent with periods of high-pressure and time sensitive activities. Attacks can be very limited and camouflaged, making them difficult to detect. Additionally, determining the potential impacts of an intrusion is not straightforward.

The user of the information is the first person affected when there is a system compromise. User behaviors may change based on the ease of their interactions with their computers. As users are continuously interacting with the systems that are monitored by analysts as well as more directly involved in the missions that would be impacted by a cyber attack on those systems, it is our contention that information about combined user behaviors should be exploited to help inform cyber operators of systemic problems. But before we can adequately make use of user behavior, we must understand it. Therefore, we propose that our cyber research strategy should include an understanding of the effects of an attack on end users.

2. The User as Sensor

Often the first impacts of a cyber attack are felt by the end user of the technology. There are many more end users than cyber defense analysts, but even if the end users are slowed down or otherwise frustrated by a problem with their computer, they do not necessarily immediately consider the possibility of a cyber attack. Think about the last time your system was slow or a webpage that you were trying to access would not load. Did you automatically assume that someone had hacked into your system? Did you immediately call the help desk or tech support? Do you believe that you should have done so?

Problems experienced by a single user are less often not the result of a cyber attack. However, users are not in a position to determine if their experiences are isolated or common with other users interacting with the same information systems. The latter could be an indicator of a cyber attack. Think about the last time your system was slow or a webpage that you were trying to access would not load. Did you automatically assume that someone had hacked into your system? Did you immediately call the help desk or tech support? Do you believe that you should have done so?

Problems experienced by a single user are less often not the result of a cyber attack. However, users are not in a position to determine if their experiences are isolated or common with other users interacting with the same information systems. The latter could be an indicator of a cyber attack. Think about the last time your system was slow or a webpage that you were trying to access would not load. Did you automatically assume that someone had hacked into your system? Did you immediately call the help desk or tech support? Do you believe that you should have done so?
Suppose that the network within which a user’s computer resided was monitored by an automated system. Suppose further that the automated system could sense when that user became agitated or frustrated as that user interacted with his or her computer. Of course there are many reasons why a user could be agitated or frustrated, but now suppose that the database he or she was accessing was also being accessed by other users on the network, and a large portion of those users were also displaying signs of agitation or frustration. The combined information could be used by the automated system to suggest that there is a potential problem with that database. As an individual using the computer, the user would probably have been unsure as to whether it was his or her computer, the network, the database, another application, or something else that causing the problem and may simply have decided to try again later or perhaps just cope with the frustration. If he or she had known that others were having the same problem, the user might have reported the problem or might have just assumed that it had already been reported. If the technology was in place that could monitor and correlate user activity and behavior, that system could not only automatically report potential problems once some threshold is met but could also inform the computer analyst of which users were being impacted.

3. Understanding Interactive Behavior

In order to capitalize upon user behaviors, more must be understood about how cyber attacks are likely to affect user states and also how those state changes are manifest in interactive behavior. We believe that this relationship is not straightforward and is likely to be mediated by individual characteristics and experience among other things (see Fig 1). Our lab has recently begun a research program to explore these relationships and more completely develop this model.

4. Conclusions and Future Directions

It is important that we understand the role and needs of Cyber Defense Analysts and develop tools to assist them in their work. We propose that, although it is critical to conduct research focused on Cyber Defense Analysis, research should be extended to investigation of impacts of cyber attack on end users. Knowledge gained in this area could yield information that not only provides analysts with more timely warnings of potential intrusions, but could also help them to determine impacts of those intrusions upon the larger mission.

We have proposed a descriptive model of the effect of cyber attack on user performance and suggested some of the potential relationships. We believe that it is important to further develop and validate this model and to go beyond description to attempt to understand the mathematical relationships among its components to support its practical application. More must be learned about the validity and reliability of such measures in operational environments. Additional research should be conducted to support a greater understanding of the relationships and trade-offs between predictive accuracy and intrusiveness.

Acknowledgements.
Our current (on-going) research program is an in-house effort by the 711 Human Performance Wing, Air Force Research Laboratory (AFRL). We are grateful for AFRL Wright State University and the Air Force Institute of Technology for their support.
References


