ABSTRACT

Network is a mix of healthy, potentially vulnerable and already infected hosts. One would always want to keep the already infected as well as potentially vulnerable hosts separate from healthy hosts. The objective behind this is to stop transitive spread of vulnerability from one infected host to another and also prevent potential attack on other shared resources. Network admission solutions try to solve the problem of keeping such hosts in a separate functioning section from clean hosts. Network administrators normally prevent the vulnerable and infected hosts from accessing resources outside the network periphery, in lieu of the fact that they may launch an attack on outside resources which may backfire on the network performance itself.

Along with applying these rectifying methods, one would also want to prevent such incidents from happening by protecting potentially vulnerable but not infected applications either by restricting access. Most of the solutions implement this security by denying access of admission of such potentially vulnerable or infected hosts into network and by restricting overall network as well as Internet access for them. This implementation may effectively work if we considered every potentially vulnerable host as infected hosts. We categorize potentially vulnerable host and an infected one as: A windows machine running with lower service update version is considered as potentially vulnerable but a machine having a virus is an infected host. Tight security restrictions in organization may lead to productivity loss if absence of security update prevents a user to access official mails.

Our research is a concentrated effort to maximize alert capturing with context information, simplify alert aggregation using a novice approach, without compromising with network performance. We propose a model that can be as secure as conventional solutions without compromising network productivity. The proposed model advocates the fact that not the machine but the application running on that host is either potentially vulnerable or infected so the access control policy focuses on the process and not at a gross level of host. The model is designed to keep the compromised applications separate from clean applications. It also builds up the run time data information for such applications running in the network to maintain the global black list of such applications with highest confidence level. Our research also generates precise set of advices to network administrator for attack prevention in real time.
Acknowledgement and / or Dedication

Endless thanks go to Lord Almighty for all the blessings he has showered onto me, which has enabled me to write this last note in my research work. During the period of my research, as in the rest of my life, I have been blessed by Almighty with some extraordinary people who have spun a web of support around me. Words can never be enough in expressing how grateful I am to those incredible people in my life who made this thesis possible.

As they say, any journey cannot be accomplished without the able support of people who directly or indirectly lend their time or resources, in order to reach your goal. First and foremost, I would like to convey my heartfelt gratitude to my parents, my husband, my son and my entire family for their continuous motivation and adjustments during this crucial tenure.

I would like to thank from the bottom of my heart to my supervisor Dr. Bhushan Trivedi, for believing in me, even when I gave up from time to time. His blessings, motivation and constant support in worst and best times, has finally paid off in terms of our research. It would not have been possible for me to constantly strive for better performance without his extraordinary vision. As a teacher and a guide, he never leaves the hands of his students. He is with you like a shadow during good and bad. He has always believed in me more than anyone else. I would also like to sincerely thank Dr. Pramode Verma, Dr. Haresh Bhatt and Dr. D.B. Choksi for their frank reviews and suggestions which made our journey a lot easier.

I would like to address special thanks to the unknown reviewers of my thesis, for accepting to read and review this thesis. I wish to thank the authors, developers and maintainers of the open source used in this work. I would like to appreciate all the researchers whose works I have used, initially in understanding my field of research and later for updates. I would like to thank the many people who have taught me starting with my school teachers, my undergraduate teachers, and my post graduate teachers.

Last but not the least; I would like to thank Cyberoam Technologies Pvt. Ltd. for providing
us with industry support for developing our research prototype model and also for funding our patent filing procedure. A special thanks to Mr. Jimit Mahadevia, for his able inputs and technical guidance, which made our research industry compliant.