Abstract Updating systems for security vulnerabilities has become a cumbersome yet necessary evil in today’s environment of zero-day exploits and ever-changing threat matrix. The current state of affairs for the vulnerability and threat management functions are in dire need of a solution that can rapidly assess systems for vulnerabilities and fix them expeditiously. This will guarantee the effective reconnaissance of critical vulnerabilities in a more concise and cohesive fashion throughout all industries affected by the inherent risk in systems and applications. This will also help defend against super-fast worms and other malicious mobile code that can blaze through an organization’s network leaving a path of compromised systems and reduced availability. The top-down centralized model for vulnerability assessment and remediation has proven inefficient and riddled with multiple vulnerabilities itself; the irony is befuddling. In this paper, we propose a framework to enhance an organization’s information security posture by distributedly assessing and remedying system vulnerabilities. By creating and utilizing the proposed framework, we can ensure more vigilance, a progressive and reactive implementation of a patch-management and worm defense strategy, and increased efficiency in the distribution of updates. Malicious mobile code, specifically worms, are very efficient in their distribution, this is because they are able to infect other systems in a peer-to-peer distributed fashion. By utilizing a similar approach to vulnerability assessment and patch management we can ensure a higher coverage and redundancy for all systems within and organization. The framework proposed in this paper is timely since most peer-to-peer distribution models focus more on content delivery and resource allocation.

I. INTRODUCTION

M ost security vulnerability assessment products detect system vulnerabilities based on signatures and complex heuristics that can identify the software revision and services running for various computer systems and their associated services and applications. Vulnerability assessment and patch management products rely on these methods to identify system vulnerabilities on an on-going basis. The patch management systems then invoke a series of patches based on the system vulnerabilities identified. Oftentimes, these systems offer a top-down centralized approach that is inherently insecure and unreliable [23]; remove the head and the giant surely falls. Progressive and reactive vulnerability assessment and patch management is a necessity to protect organizations from zero-day exploits, worms, and hackers. We need to expeditiously assess for system vulnerabilities and remediate systems efficiently in order to protect organizational brands and shareholders against potential financial loss. This paper will describe a framework for successfully utilizing a distributed approach to remedy system vulnerabilities.

II. LITERATURE REVIEW

A continuing review of the literature on vulnerability assessment and patch management finds no mention of the idea of distributedly assessing and remedying system vulnerabilities [1]-[39]. Effective vulnerability assessment and security patch management is critical to defending against malicious mobile code, yet despite its importance very little has been written on the processes that organizations use to implement patch management [9]. The health of the patch management is critical to an
organization’s information security posture; as such vulnerabilities must be found and eradicated expeditiously [15]. Vulnerabilities are most commonly known for their penchant of becoming exploitable by nefarious parties. Predominantly, they are identified by (1) company specific application researchers, (2) independent security researchers, and (3) hackers. The current process of vulnerability reporting is primarily characterized by the collaboration of independent and company specific application researchers. The secondary aspect of vulnerability reporting, or lack thereof, is characterized by hackers creating exploits for nefarious reasons, such as: gaining access to, taking control of, disrupting functionality of, and/or destroying information from unauthorized systems. System vulnerabilities are most commonly found by information security researchers and company specific application researchers. The fixes to these vulnerabilities follow a methodical disclosure and remediation lifecycle that endeavors to maintain the security and usability of the vulnerable system / application. When hackers are first to ascertain a possible vulnerability in a particular system / application, they quickly create an exploit and try to commandeer any affected system they can reach in a short period of time, these are known as zero-day attacks. Zero-day attacks are an uncommon but prevalent security problem. Notwithstanding, hackers are active participants in the normal remediation lifecycle; by patiently awaiting the release of a vulnerability fix they then reverse engineer this fix to create malicious code, e.g. worms, to enact their nefarious intent. This poses a great risk for computer systems and it is within this small window of opportunity that this paper will focus on. Why does this problem pose such a great risk? Once a critical fix is created by an application/system vendor, the fix must be applied expeditiously to ensure minimal risk and exposure within an organization’s computer systems. For example, there’s critical fix for the Acme Word Processing program, this fix mitigates the vulnerability that allows a remote attacker to completely take over a vulnerable machine. ABC Corp. identifies 10,000 systems that are vulnerable within its organization. Like most organizations, ABC Corp. has a centralized vulnerability assessment and patch management system that it will use to distribute the fix. Unfortunately, the ABC Corp. could not assess all 10,000 systems, let alone fix the vulnerabilities expeditiously, this lead to a massive outbreak within its network. Identifying system vulnerabilities and patching expeditiously is one of the critical elements of patch management [19] that can be used to ensure a heightened information security posture, ensure compliance with organizational policies, industry best practices, certifications and regulatory mandates. Despite vulnerability assessment and patch management’s importance, practitioners have few available resources to help them implement and effective process in large scale environments. This makes them even more susceptible to malicious mobile and rapid spreading worms. This is the area where my research and framework will have its biggest impact. The framework proposed in this paper will enable the distributed assessment and vulnerability fix of all systems within an organization. The approach is based on P2P networking and distribution but with system specific extensions for the vulnerability assessment and patch management capabilities. The peer-to-peer approach presents us with the possibility of extending and harnessing idle storage and network resources from client machines that are part of an organization’s network. The benefits of peer-to-peer networks are numerous e.g., performance, availability, and fault-tolerance. Participants in this extended peer-to-peer framework will serve as resource providers and operate autonomously once a critical fix is assessed and the appropriate fix is identified and mandated by the organization’s information security department. Since we are building on a peer-to-peer networking approach, the inherent redundancy will increase the availability and the speed at which systems are assessed for vulnerabilities and remedied. This will greatly decrease the vulnerability lifecycle process and, according to Brumley et al, it is one of two strategies that hold the most promise for protecting against new ultra-fast smart worms [8].

III. SUBPROBLEMS

By distributedly assessing and remediying system vulnerabilities we can increase operational efficiencies, increase an organization’s security postures, and increase the speed in which patches are deployed. This methodology is novel as vulnerability
assessment and patch management frameworks do not utilize a distributed approach; they utilize a top-down centralized approach; this approach can be either manual or automated [19]. These systems leave much to be desired, specifically for worm infestations that can cripple organization’s network due to their high infection rate. There is an ever existing shrinking interval from the time a new vulnerability is announced and the time a worm or malicious mobile code exploits it. The proposed framework will retain focus on vulnerability assessment and remediation to avoid pitfalls of network-based defense techniques. This will be a reactive solution similar to the Reactive Antibody Defense [8]. Currently, it is also very difficult to attain high-levels of effectiveness in vulnerability assessment and patch management. How can a distributed framework increase the effectiveness vulnerability assessment and remediation and enhance and organization’s security posture? Increase operational efficiencies and decrease or eliminate single-failure points [8], [9], [23]? These questions will be directly addressed by implementing his practical framework and approach. The specific extensions developed to assess vulnerabilities in this framework need to automatically report any known vulnerabilities to all the peers within its range and subgroup. These vulnerabilities will then be aggregated and distributed to all nodes participating in the organization’s peer-to-peer network. Concurrently, any peers found to be vulnerable will be immediately patched for by its peers. Peers will proactively identify all members that are non-compliant, vulnerable, and immediately push the fix distributedly, greatly reducing the time required for covering a large scale network and eliminating single failure-points.

IV. ASSUMPTIONS

The methodology/system described in this paper will serve as a catalyst for changing the way that vulnerabilities are assessed and patches are distributed. This should be beneficial for both corporate and consumer entities. Participating systems must be part of a trusted security domain, such as Microsoft Active Directory, LDAP, or a secure network environment, e.g. within an organization’s intranet. The security domain should be pervasive enough to accommodate distributed peers and distributed updates in a fast-paced evolving environment. Un-trusted systems are inherently prohibited from participating in this model. The extension to the peer-to-peer model will make this framework system agnostic, providing coverage in a heterogeneous environment; this is what is usually encountered in large scale organizations. Systems should be located in a structured network environment for best results; the capacity modeling for this framework will be performed under optimal network conditions, mimicking a global and distributed organization. The current peer-to-peer agent of choice is the BitTorrent client. This will allow for appropriate modeling scenarios, since BitTorrent traffic accounts for a large portion of traffic on the Internet.

A. Significance

Distributedly remediying systems vulnerabilities in a distributed environment is primordial to a progressive and reactive vulnerability assessment and patch management program. The research described in this paper will result in the following: Development of framework/methodology for successfully utilizing a distributed environment that will allow for pervasive vulnerability assessment and patch management whilst minimazig speed and reducing the security exposure of the environment and its associated peers. This will in turn increase operational efficiencies in the patch management process whilst minimizing or eliminating single-failure points. Create the foundation for establishing a distributed environment for any type of data sharing and content distribution systems where assessments and updates are required.

B. Methodology

The goal of this research is to provide a distributed vulnerability assessment and patch management program within any computing environment to ensure that system vulnerabilities are remedied in an expedient and efficient fashion whilst minimizing system overhead and operator intervention when remediying the detected vulnerabilities. This will be accomplished by extending the peer-to-peer networking environment to include localized system assessments and fix installation. This distributed environment is primordial for the assessment of vulnerabilities and the distribution
of patches to minimize the risk exposure of vulnerable systems and, ultimately, increase an organization’s security posture.

For this research to be effective, a proper foundation must be in place in order to ensure the confidentiality, integrity and availability of systems whilst maintaining a robust security environment.

C. Procedures to be employed

The specific procedures to be employed are based upon the creation of a new paradigm model of assessing vulnerabilities and distributedly remediing systems. Empirical and theoretical scenarios will be undergo a discrete and practical meta-analysis that will facilitate and clarify the following dependent variables necessary for validating the importance of this work: increase in organizational security posture by distributedly remediing system vulnerabilities, increase the operational efficiencies associated with the vulnerability assessment and patch management process, decrease or eliminate single-failure points. Assessing a large scale computing environment to ensure systems have the prescribed level of security fixes. The dependent variables involved in this approach are characterized by the inability in current systems to ascertain and distributedly patch vulnerabilities in an organization’s environment. This meta-analysis will allow for further refinement of the hypotheses and define the theory of increasing speed, increasing security posture, and eliminating single-failure points in the vulnerability assessment and patch management process by extending the current peer-to-peer networking model.

D. Projected outcomes

The projected outcome of this research will ensure that systems can be proactively assessed and patched for vulnerabilities in a distributed fashion; ensuring that any vulnerabilities identified by any peer are collectively remedied in a timely fashion by all peers within a networking environment. This will raise the security posture of any organization where this system is implemented. A practical and functional peer-to-peer system will demonstrate the necessity of such as system and validate the hypotheses made. The empirical data will help quantify and solidify the necessity of such a system in our current environment of ever-evolving threats and zero-day malicious mobile code attacks. The system will deal with the risks associated due to catastrophic failures within the environment and efficiencies built to mitigate these special circumstances.

V. CONCLUSION

The ever-changing landscape of vulnerability disclosures and exploit creation by malicious attackers leaves many organizations and information security teams with limited option for remedying them and ensuring that their client systems are in compliance to corporate policies. Furthermore, when responding to fast spreading malicious mobile code, organizations and information security teams are currently the loosing the battle [19], [24], [28]. A shift from a centralized approach to vulnerability assessment and patch management is necessary to keep-up with the techniques utilized by malicious attackers. Recent worms and other malicious mobile code are able to infect machines without using a centralized repository; they scrumptiously infect machines at a very rapid pace. Organizations are unable to keep with many of these malicious code outbreaks once they have penetrated their internal networks. By successful representation the security benefits of distributedly assessing and remediing system vulnerabilities and empirically demonstrating the benefits via scenario based analyses we can promote a better information security posture for all environments where the proposed system/methodology is implemented. The quantifiable empirical data considerations needed to support the independent and dependent variables of this research will be showcased by the extension of the peer-to-peer networking model to include assessment and patching capabilities to bring forth the proposed framework and system.

The practical applications of the findings will be directly beneficial and applicable to the security postures of businesses and organizations worldwide. The findings will greatly enhance the security posture of the businesses and organizations where the system is implemented. This research is revolutionary in its simplicity because it attempts to use techniques similar to those used in infecting and exploiting system vulnerabilities [8], [17].
This research will focus on quantifying the security benefits achieved by distributedly assessing and remedying system vulnerabilities by performing a meta-analysis of the gathered empirical data and previous research on peer-to-peer networking, content distribution, worm propagation and defenses, and patch management. The goal of this study is twofold, the creation of a framework that is conducive to creating more secure computing environment by timely and efficiently assessing and remedying system vulnerabilities and quantifying the increase and organization’s security posture by progressively and reactively defending against fast spreading malicious mobile code.

The current recommendations for additional studies include: creating a trust-secure model for system/package tasks; managing data distribution paths within a trust-secure environment; optimizing traffic vectors for seamless data distribution within large-scale environments; extending a peer-to-peer networking model for pervasive systems monitoring and management. The contributions to the field of study will be numerous and will greatly enhance the common body of knowledge by creating a framework that is scalable and applicable to many problems that relate to the assessment and remediation of subjects that are known a priori.

ACKNOWLEDGMENT

The author would like to thank Dr. Fran Gustavson, his dissertation advisor, for her valuable discussion and input. The author would like to thank his dissertation committee for providing guidance and feedback. The author would like to thank Dr Nagaraj Rao and Dr. Zhixiong Chen for their valuable feedback and input.

REFERENCES


[18] M. Gegis and L. Williams, "Matching attack patterns to security vulnerabilities in software-intensive system


