Chapter 29
A Security Framework for Enhancing User Experience

Van Nguyen
Department of Computer Science, Saint Leo University, Saint Leo, USA

Marwan Omar
Department of Computer Science, Saint Leo University, Saint Leo, USA

Derek Mohammed
Department of Computer Science, Saint Leo University, Saint Leo, USA

ABSTRACT

In this paper, we present a novel framework that enhances user experience for their daily computing activities while being protected from cyber threats. The conceptual security framework also targets two additional goals: enabling end-users to experiment software applications before making a decision for a real installation, and serving as a testing environment for both research scholars and security practitioners to analyze and predict potentially malicious activities. The framework introduces three modes of operations (full lockdown, partial lockdown, and administration) and a virtual storage that provides a safe, secure, and reliable computing environment for end-users. We also present three use cases that show the applicability of their framework in a real-world environment.

INTRODUCTION

A good end-user experience includes many aspects such as a clean interface, an easy to navigate control, or the flexibility to operate a computer without fear of harmful threats. The flexibility also permits using the computer without hindrance, which can be restricting the installation a computer software, enabling cookies, or changing the configuration of the operating system or software. Rosenzweig (Rosenzweig, 2015, p. xv) states that "the goal of user experience is to design products that are less prone to human error." Human error can contribute to oversight, lack of software knowledge, or unintended actions. A simple click of a mouse can cause great consequences if the system does not have a strong protection.

DOI: 10.4018/978-1-7998-7705-9.ch029

An example of a great consequence can be drawn from the Flame virus attack (Munro, 2012). The virus infiltrates a system and fakes Microsoft digital security certificate to download updates. The updates look legitimate but indeed masquerades spyware.

A counter to errors (human and software) is to restrict user access (read/write) to the system. However, it has drawbacks in providing this type of system security to end users. If a system locks down most of its filesystem access or modifications, the users would not be able to install programs, make changes to the configurations, or even have access to cookies in the Web browsers. Thus, the user experience is compromised as more restrictions are placed on the system. In Microsoft Windows operating systems (MS OSes, prior to Windows XP), there were no restrictions at all except a warning before making deliberate or inadvertent modifications to system files (Anderson, 2001). This is due to the fact that these Windows OSes gave full administrative permissions to users by default. The later versions of MS OSes implemented more rigorous access control mechanisms. At the other end of the spectrum, Linux operating systems implement a mandatory access control mechanism that could lock out all modifications to system files and application files.

The usage flexibility provided in modern operating systems (Windows, Linux) allows the users to change the access control within the operating environment: the users just need to provide the appropriate credentials. But this implementation has a big drawback that allows applications installed without the ability to test whether they are safe or they meet the user's criteria requirements. Another drawback is even though we can have the ability to uninstall them, some applications allow users with average computer skills to install but require their expert computer skills to uninstall, for example, Oracle database, anti-virus software, or self-healing spyware (Wu e. a., 2007). This is the main drive for our framework. The ability to test out applications before making the decision to install the applications. In this way, the users do not need to compromise their computer system configuration or security.

Security versus Convenience

Security professionals are facing growing dilemmas as they strive to secure their networks while trying to simplify access to network resources for authorized users. The 'lock it all down' principle can no longer be achieved as networks become more interconnected and more legitimate users need to access digital resources to stay productive and efficient. As security practitioners try to defend networks and secure them against hackers, they are faced with the dilemma of providing smooth and seamless access to legitimate users, this is where security and convenience may collide resulting in either disappointed users or potentially leaving doors open for hackers to break into networks and ultimately steal sensitive business information. These information security infrastructures are being modeled after Fort Knox without taking into consideration how such stringent security measures may impact end-user productivity and performance (SANS, 2004).

The core issue lies at the fact that end-users want easy access to information resources to make their job efficient and productive while security professionals have the responsibility of securing networks from unauthorized access and ultimately preventing unnecessary attacks. This dilemma represents one of the unique challenges for security practitioners where they have to strike a balance between security and convenience; they are required to harden networks with security tools and measures and still enable users to smoothly access the resources they need to achieve their daily business tasks.