



‘Out of Band’ Protection: Fault proof method of protecting End-user data from key loggers, malicious software and Trojan horses

Introduction

Consumers increasingly want to access their accounts from anywhere, at anytime. However, the convenience of checking balances, paying bills and transferring funds online leads to substantial risk. Accessing these accounts from public kiosks in airports, train stations and Internet cafes is fraught with the danger of keyboard loggers recording what consumers type, including usernames, password and bank account and credit card numbers. Armed with this information, criminals can empty a consumer’s bank account.

Malicious software that is secretly installed on PCs can record the keystrokes used to type user IDs and passwords for accessing online bank and other confidential accounts. It also can capture screens — thus, mouse-clicking passwords on an on-screen keypad also is not secure, although capturing screens is more resource-intensive for criminals to do than logging keystrokes. Keylogging and other eavesdropping software can be installed locally by cyber thieves (such as on a computer at a cyber café or university computer room), or by viruses and worms that install the software over the Internet. Malicious software often arrives as "Trojan horses," which look like legitimate applications and eavesdrop on user actions. The increasing incidences of these attacks threaten the safety of consumers' communications, information and relationships with online service providers, such as banks, healthcare providers, retailers and payment processors.

Banks and other e-commerce providers can minimize problems from keyboard logging by preventing connections from unknown machines. However, this is a Draconian measure that eliminates the convenience of accessing online services from anywhere, at anytime.

What are Keyloggers

A Keylogger – often called as Keylogger, Key Logger, or Keystroke Logger - is a program that runs in the background, recording all the keystrokes. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped raw to the attacker. The attacker then peruses them carefully in the hopes of either finding passwords, or possibly other useful information that could be used to compromise the system or be used in a social engineering attack. For example, a key logger will reveal the contents of all e-mail composed by the user.

Calling for new security requirements

The current paradigm of security emphasizes network level protections that keep hackers away from accessing the corporate systems through the networks. These solutions are centered on protecting/filtering network traffics from bad guys getting into the domain. Even though virtual network connections such as Secure Socket Layer (SSL) and VPN technologies promoted network security at a higher level, new schedules of security threats have exposed a security gap existing at the client machine. This security gap has not been addressed by most corporate security officers, because most of the security threats and attacks center on illegal intrusion to restricted domain access and hacking information within.

This security hole existing at a remote client machine poses new security threats and even further elevates to attacks on an end-user's identity. This threat has immediate financial impact on end-users and yet it could bring more detrimental impact on large enterprise/government users as well.

What are the pros and cons of current anti-keylogging tools

PC Scanning Programs

PC scanning programs look for malicious programs, files or processes, such as keyboard loggers, by using signature-based or behavior-based software.

1. Signature-based scanning programs

Signature-based programs include standard antivirus scanning software. This approach is limited regarding keyboard logging detection because antivirus software is only as good as its last update on a customer's PC. The update has to recognize the signature of the virus that is used for keyboard logging. In addition, signature based programs take a long time to download — typically at least 15 to 20 minutes over a high-speed line. Once loaded, the program automatically scans the files on a PC, checking the signature of the file against a list of signatures known to represent malicious viruses.

Cons: These programs can't detect Trojan horses that are used for keyboard logging because Trojan horses look like normal, "friendly" programs. They are too batch-oriented and latent to be effective against viruses that may not be pervasive or that do too much damage before they are detected.

Although some anti-virus programs are able to filter out some malicious codes/spyware, it cannot detect the latest or unknown keylogging programs due to its inherent limitations of signature-based technology. A Personal Firewall can't prevent outgoing key log files, because most of the key logging programs are sophisticated enough to disguise their communications as valid network communications. Commercial keyloggers are normal registered programs, which current anti-virus software has difficulty detecting.

2. Behavior-based scanning programs

These programs scan live processes running on a desktop before a user is allowed to log into a service provider's site, such as a home banking site, to detect "sniffing" or keyboard logging software. The user initially downloads this program from the provider's site. The program generally is small (approximately 300Kb) and takes seconds to download. It lists the live processes, runs them through a sequence of tests, and checks for malicious behaviors and characteristics. For example, it looks for a process that is logging keystrokes, opening remote connections, or is small and trying to hide. This behavior is scored; if the score indicates a threat, the scanning program will terminate the process on the PC.

Cons: Users who access sites from PCs inside of corporate firewalls or other restricted environments probably will be prevented from downloading and running the requisite programs, which are typically ActiveX. In addition, protecting PCs in kiosks requires the cooperation of kiosk owners. Support or multiple platforms, such as Apple operating systems and older versions of Windows, will also be difficult.

These solutions generally work better for detecting keyloggers than regular anti-virus solutions. However, most of the anti-spyware solutions are signature based. A signature base solution has three major vulnerabilities; 1) requires frequent updates for up-to-date signature database, 2) even 'up-to-date' signature databases do not cover unknown or registered commercial key loggers, 3) It takes up client PC resources to run scan files and to monitor processes.

How StrikeForce Technologies meet the challenge

StrikeForce's GuardedID™ encrypts all entered data with 128-bit encryption to prevent hacking tools (Trojan horses, spyware and keyloggers) from stealing user information. In other words, GuardedID™ simply creates a 'local SSL' at a local user machine and delivers entered data to an application (browser) message queue through a separate channel of the keyboard

driver. The 'local SSL' is activated upon a policy decision of a corporate.

Integration of the technology is seamless. It integrates with customer's existing Internet browsers without any configurations, reboots and manual execution/terminations.

When GuardedID™ is effect, malicious programs and Trojan horses cannot recognize the presence of GuardedID™ and they are unable to tap any key events from users, because entered data is being delivered to the application queue through a different channel and is already encrypted.

Installation of GuardedID™ is completed by including an object code into a web server.

