STRIKEFORCE TECHNOLOGIES

GuardedID®

Whitepaper

StrikeForce Technologies, Inc.
1090 King Georges Post Rd.
Edison, NJ 08837
www.strikeforcetech.com

Summary

Keyloggers are a serious security threat that can be extremely harmful to both businesses and consumers. Current mechanisms do not provide adequate protection to the user from these threats. We discuss a solution that helps users mitigate the keylogging threat and show how GuardedID can prevent the information leakage to current as well as future keyloggers.

Introduction

Though PC users are worried about spyware that tracks web site visits, and crashes their PCs, there are more insidious threats out there. A more powerful breed of spyware can log keystrokes (including passwords and credit card numbers) and send that information to criminals. This type of software is called a keylogger.

A keylogger is a type of surveillance software that has the capability to record every keystroke you make to a log file (usually encrypted). A keylogger can record instant messages, e-mail, and any information you type at any time using your keyboard [4]. The log file created by the keylogger can then be sent to a specified receiver. Some keylogger programs will also record any e-mail addresses you use and Web site URLs you visit.

This danger was recently highlighted when Sumitomo Mitsui Banking Corporation discovered a keylogger installed on its network in London [1]. There have been other high-profile cases. In 2003 keylogging software was discovered at more than 14 Kinko locations in New York. The perpetrator installed the software and using it to open bank accounts with the names of some of the 450 users whose personal information he collected [2]. Also in 2003, Valve Software founder Gabe Newell found the source code to his company's Half-Life 2 game stolen after someone planted a keylogger on his computer [3].

Keylogging is a serious security threat that can be extremely harmful to both businesses and consumers. By copying keystrokes, hackers are able to access private financial information such as bank accounts, credit card numbers,

and social security numbers – all of which can be used for fraudulent activities, that you won't know are occurring until the effects show up on a statement, bill or via a phone call which could take days, weeks or months to surface.

How keyloggers are inserted into a victim's computer

A keylogger can be inserted into a victim's computer via several ways. It can be carried by a virus or spyware. It can come as an attachment in an e-mail. For example, the Corporate IT Forum spam email contains a website link, the clicking of which, causes a keylogger to be loaded into the computer. It can even be embedded in an mp3 file or delivered via a XSS (Cross Site Scripting) attack.

How keyloggers work

Keyloggers work by hooking the Windows message queue. It is relatively easy to place a hook and inspect all the windows messages (such as keystroke messages) before they are sent to the application. The keyloggers then log the keystroke messages into a file. Typically, the keylogger communicates with the hacker via an IRC channel and delivers the captured keystroke file to the hacker. Many keyloggers also incorporate stealth mechanisms (using rootkit techniques) to hide their existence so that they cannot be detected by anti-virus software.

Why current tools don't work

All anti-spam and anti-virus tools are based on scanning a computer for files with a particular signature. The database containing signatures of known bad files have to be continuously updated. The major caveat in this approach is the existence of the signature of a known problematic file. Spammers and criminals are currently deploying sophisticated software which dynamically changes the file signature. Therefore, anti-spam tools are no longer effective against keyloggers. Also, there is significant time between detecting a new keylogger on the internet and the anti-keylogging signature being updated on

anti-virus/spyware software. This time gap can take a month to a couple of months.

Some of the anti-keylogging software prevents Windows hooks from being used by keyloggers (Windows hooks are used by keyloggers to spy on keystrokes sent from the keyboard to the application). However, there are not always effective and can be circumvented by keyloggers in most cases.

How GuardedID protects users

GuardedID uses a different approach to defend against keyloggers. Rather than trying to detect keyloggers, it takes a preventive approach. It takes control of the keyboard at the lowest possible layer in the kernel. The keystrokes are the encrypted and sent to the browser via an “Out-of-Band” channel bypassing the Windows messaging queue. GuardedID has a built in self-monitoring capability. This prevents it from being bypassed by other software. If GuardedID is tampered with in any way, it will warn the user of the breach.

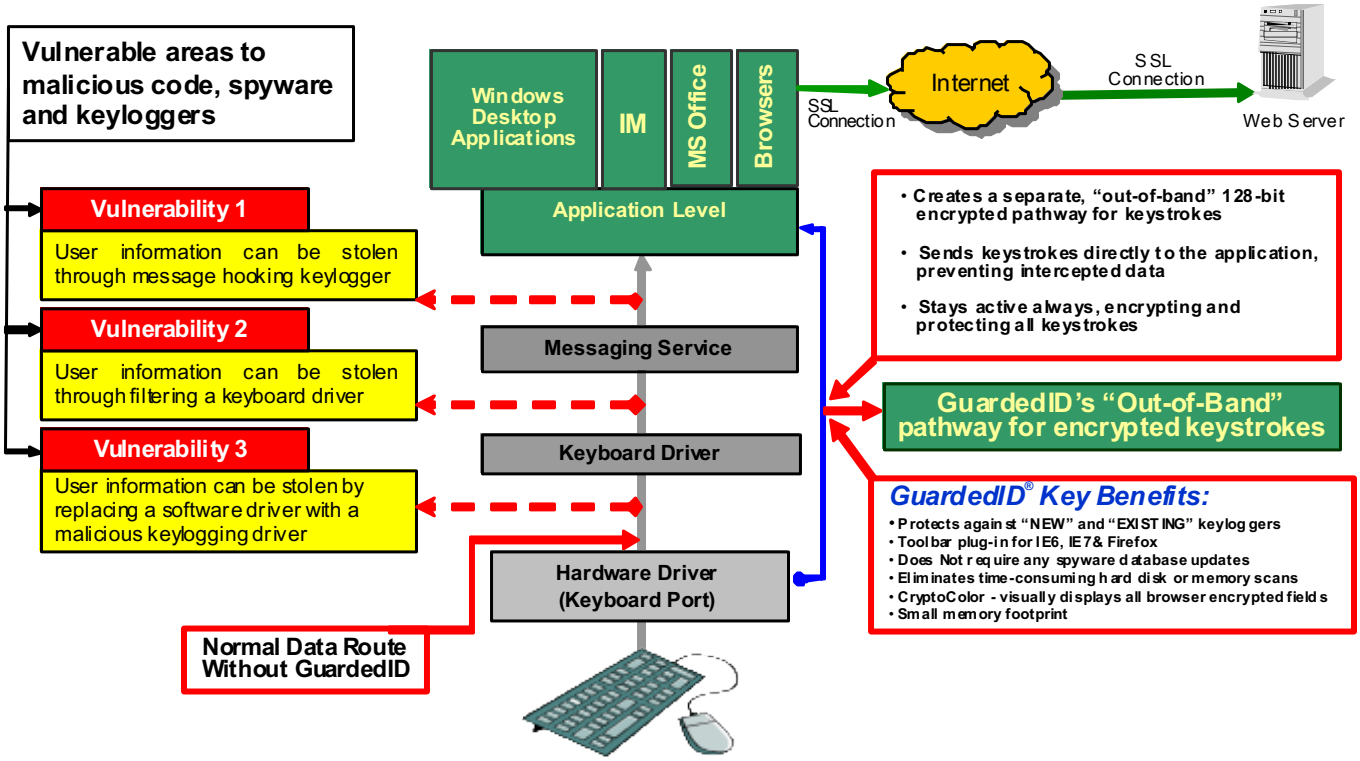

Figure 1. How GuardedID works

CryptoColor

GuardedID uses a unique method to indicate to the user that the product is working and the user input is secured. It colors the text input box that the user is entering data in. The color can be selected by the user. This provides strong visual feedback to the user that they are operating in a secure environment and their keystrokes are secure.

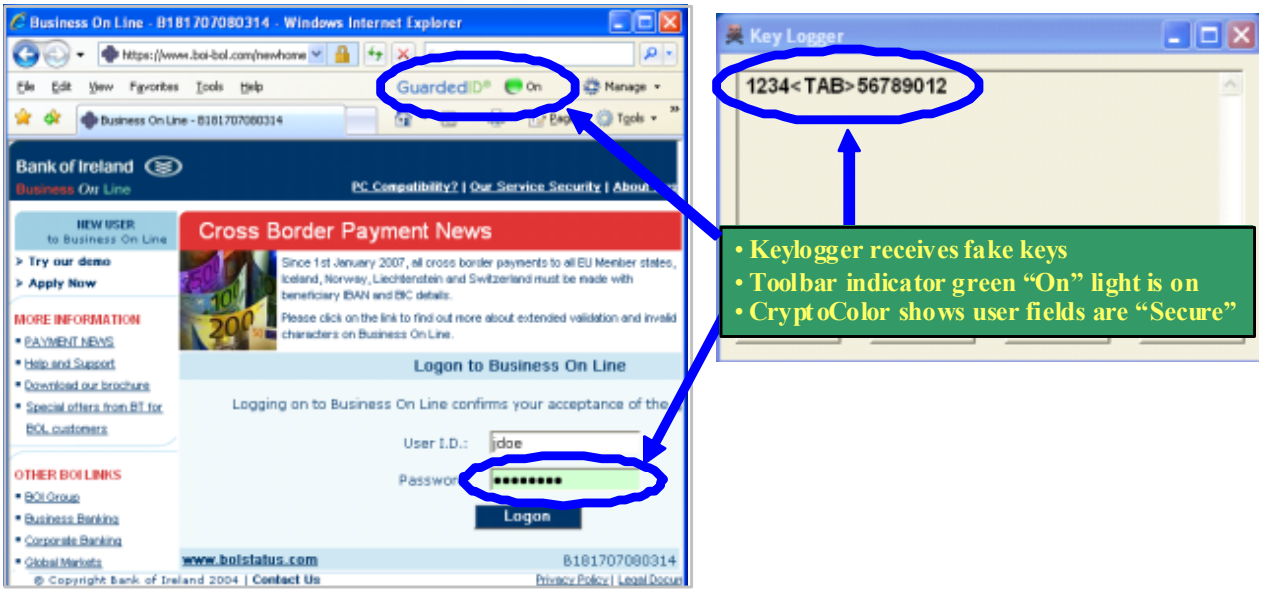

Figure 2. CryptoColor

CryptoState

In certain cases, GuardedID is not able to secure the user input. This happens with certain pages and certain types of pop-ups. In such a scenario, GuardedID warns the user that encryption is off by changing the color of a status button on the GuardedID toolbar. There are four states – (1) Activate (activate software license), (2) On (indicates that keystrokes are being encrypted), (3) Off (indicates that keystrokes are not being encrypted), and (4) Warn (indicates that an un-trusted driver has been found in the keyboard device stack)

Keyboard device driver monitoring

GuardedID constantly monitors the keyboard device driver stack to detect un-trusted drivers (which could potentially be keyloggers). If an un-trusted driver is discovered, GuardedID warns the user by showing the "Unknown Driver Warning" dialog. The name of the suspect driver is displayed in the dialog. The GuardedID state indicator will turn orange instead of green to indicate warning. Details are logged into the event log which can be viewed.

Anti-Clickjacking

Clickjacking is a new vulnerability that has recently surfaced. Web coding allows a single web page to be constructed from different items (ads, images, links, etc.) in "frames". Normally, the frames all come from a single domain (like guardedid.com) but they may come from other domains (ad servers, media servers, etc.).

Clickjacking uses this normally helpful feature to trick users by showing the expected web page but overlaying or underlaying some other unexpected page from a different domain. As a result a web page can have a hidden frame that contains a clickable button that can invisibly hover below the user's mouse, so that when the user clicks the mouse, they inadvertently click the invisible button, causes an undesirable action, such as, downloading malware, transferring money, buying something, etc. The only solution that works, in some cases, is to disable JavaScript …. something that will drastically reduce the usability and the internet experience.

GuardedID anti-clickjacking feature takes another approach. It looks at the webpage and warns the user when content is not from the same domain. If false content is hidden in an invisible overlay, GuardedID makes it visible. If the content is hidden underneath, GuardedID draws red borders around it. Either way, the user can be fully aware of the content and then be cautious of his/her movements on the page.

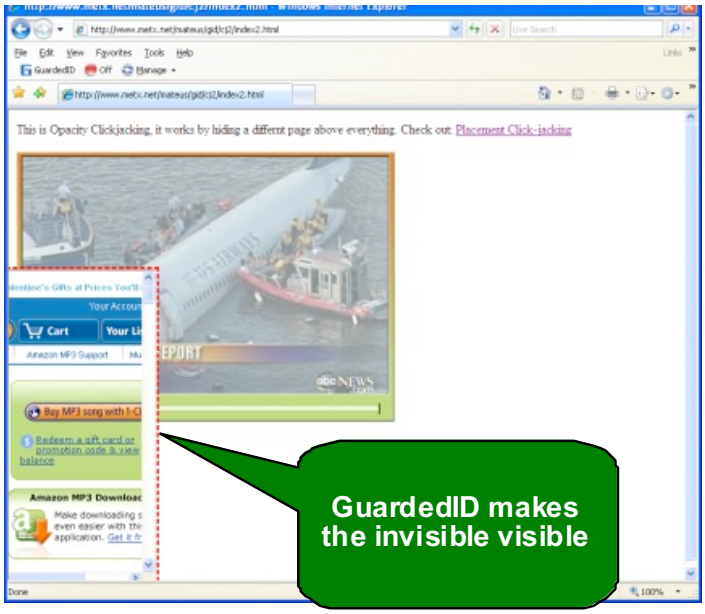

Figure 3. Anti-Clickjacking

Competitive analysis

The following table shows a comparison of GuardedID to other anti-keylogger products.

Other Anti Keylogger Products	Guarded ID
Blacklist/ whitelist based	Windows systems internals based
Requires updates on a regularly basis	Does not require updates
Retroactive defense based	Pro-active defense based
Does not encrypt input	Encrypts all input to programs
Circumvention very easy by manipulation of file names and sizes	Very hard to circumvent
	"Out-of-band" keystroke encryption
	CryptoColor

	CryptoState
	Keyboard device driver monitoring
	Anti-Clickjacking

Table 1 GuardedID features comparison

GuardedID is available in the following versions

Standard - Secures a users entire internet experience - In this scenario, GuardedID is automatically launched every time the browser is opened for any type of online activity i.e. banking, shopping, browsing, email etc. As a consumer, this option requires the user to download and install the GuardedID toolbar into their internet browser.

Premium - Secures a users entire internet experience as well as most Windows applications (such as Microsoft Word/Excel/etc., IM/chat, financial/accounting applications and many other applications) – This option includes the functionality of the Standard version.

Enterprise - Secures a users entire internet experience as well as most Windows applications – In this scenario, GuardedID is purchased and distributed by a corporation to its employees to protect all activities whether on a corporate network or working remotely. GuardedID can be distributed via a Group Policy (GPO) installer by the System Administrator. Great for corporations, government agencies, banks etc.

References

1. "Keyloggers Foiled In Attempted $423 Million Bank Heist", Gregg Keizer, Security Pipeline http://www.securitypipeline.com/showArticle.jhtml?articleID=159901843
2. "JuJu, Kinko's, and the "Keystroke Caper"!", TechSpot http://www.techspot.com/news/6478-JuJu-Kinkos-and-the-Keystroke-Caper.html

3. “Popular computer game code stolen by hackers”, Paul Roberts, Computer World http://www.computerworld.com/securitytopics/security/story/0,10801,85845,00.html
4. “Definiton: Keylogger”, Webopedia <http://isp.webopedia.com/TERM/K/keylogger.html>