



Technology & Application Review

November 1, 2007

Contents

1. Introduction

2. Architecture

3. Mechanism for Authenticating User Credentials

4. Authentication & SSL Integration

5. Applications

- Remote & Mobile Corporate Network Users

- Web Server Customer Service Costs Containment

- Financial Service Providers

- Personal Internet Security

- Healthcare

- Media Distribution

6. Conclusion



1. Introduction

Chris Rouland, CTO of IBM's Internet Security System Group, recently was quoted saying that "when it comes to security for PCs, Give up ... In the next generation we will all do business with infected end points ... How do you secure a transaction with an infected machine? Whoever figures out how to do that first will win."¹

Secure-Surfer, LLC has figured this out! Its solution provides "Safe Internet Access For Everyone, From Everywhere, Every Time[®]". **It is safe for everyone** because it protects against all possible online safety concerns including phishing, man-in-the-middle and man-in-the-browser attacks as well as keyloggers, and malware downloads. **It is safe everywhere** because it is effective even when accessing the internet from PCs infected with viruses, worms and other malware or using tapped internet connections. **It is safe every time** because it guards even novices practicing unsafe surfing habits or faced with novel social hacking techniques.

Secure-Surfer, LLC's first offering is a Web 2.0 Managed Service called **Secure-Surfer[™]**. This service is accessed using portable USB "thumb drive" keys, each unique to its user. On inserting the key into a PC the user is instantly provided with a **safe** web browser. Secure-Surfer, LLC brands and tailors **Secure-Surfer[™]** for enterprises seeking to provide safer and more convenient access to their web content and services. Secure-Surfer, LLC can brand its keys for these enterprises, tailor these for navigating exclusively to only one or a few web sites, and distribute these through the mail. As happens with credit cards, customers activate their keys by placing a phone call upon receiving their key. On inserting their key into any PC connected to the internet, customers are immediately presented with the issuing enterprise's on-line web site (e.g., online bank) and need only click their PIN number on a virtual keyboard to securely and conveniently log on. While conducting on-line banking, the user can continue using other PC applications and on removing the key their **Secure-Surfer[™]** online session terminates. **Secure-Surfer[™]** keys are available in different form factors, including credit-card shaped carrying convenience.



The demand for stronger internet web browsing security protection cannot be overemphasized. This demand is driven by the increasing use of the internet for e-commerce,

¹ Berinato, Scott. "Hacker Economics 3: MPACK and the Next Wave of Malware." CIO. 8 Oct. 2007. 1 Nov. 2007 <http://www.cio.com/article/135551/Hacker_Economics_MPACK_and_the_Next_Wave_of_Malware/2>.



online banking and other activities requiring the confidential exchange of information.² It is further accentuated by the increasing threat of a myriad of internet fraud techniques, such as phishing, key logging and man-in-the-middle attacks.³

Protection against internet fraud is principally achieved by ensuring that parties communicating over the internet are indeed whom they say they are and by protecting the privacy of these parties' communications. Today's most widely used means for achieving this protection is Secure Sockets Layer (SSL), a network protocol for managing the security of a message transmission on the internet. SSL authenticates the identity credentials of users (clients) browsing the internet and of the web sites (servers) visited by these users and protects the privacy of these parties' communications using encryption. SSL is the preferred means for providing online protection because it is inexpensive to deploy and easy to use and maintain.⁴

While SSL is effective, it ONLY provides protection from malicious attacks initiated from outside the client's PC system. In other words, SSL assumes that the end client PC system is trustworthy or free from malicious code infections (malware). Malware, though, can render SSL ineffective because it can completely duplicate client authentication credentials (such as the user's private key or password) and send this duplicate to malicious hackers. These hackers can then use the duplicated credentials to impersonate the user.

To combat against malware infections, PCs are typically protected with anti-malware software products produced by firms such as Symantec and McAfee to detect and eliminate this malicious code. Although anti-malware products have improved significantly and succeed in protecting against many malware attacks, they are nowhere close to eliminating all malware. These products are based on *signature* or *fingerprint filtering* techniques that are only effective against "known" malware. These signature-filtering techniques do not provide full protection because they are always catching up with new malware. In particular, they are unable to provide protection against new malware between the time that new malware starts infecting PCs connected to the internet and the time that PC users receive upgraded anti-malware software capable of recognizing and destroying this new malware. Closing this gap is particularly difficult because hackers are spreading about 20 new malwares daily on the internet and it usually takes a few hours to develop and distribute antidotes against newly detected malware.⁵ Moreover, as the table below shows, the inadvertent downloading of malware from the internet by PC users has become practically unavoidable.

² About 17% or 1.1 billion of the world's population uses the internet today and this usage is expected to triple over the next five years. See www.InternetWorldStats.com.

³ For more details on the growth of internet security threats see [Symantec Internet Security Report, Vol. XII, Mar. 2007](#). For more details on the cost and pervasiveness of online fraud see: Lawrence Gordon, Martin Loeb, William Lucyshyn and Robert Richardson, [CSI/FBI Computer Crime and Security Survey](#), Computer Security Institute Publications, 2006.

⁴ This security is also achievable using so-called strong-authentication solutions that use biometric readers or changing password dongels. Strong-authentication techniques are used for specialized applications and are typically not considered solutions for the internet-user population at large because they are expensive and difficult to use and manage.

⁵ [IBM Internet Security Systems X Force, 2006 Trends & Statistics, January 2007](#).



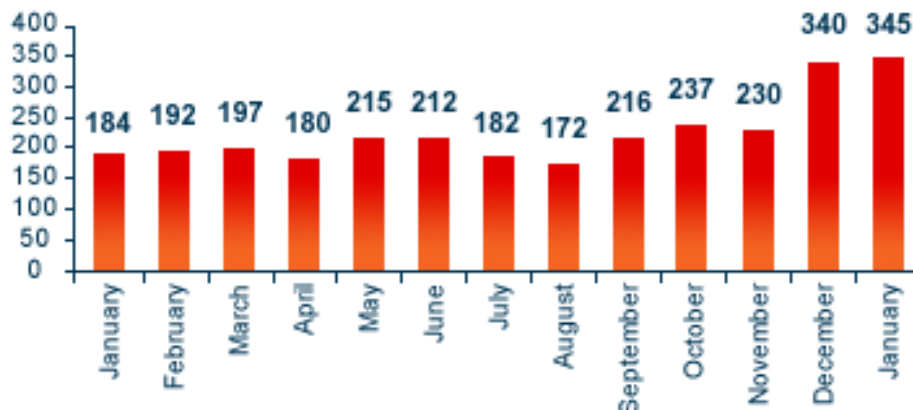
Malware Infections per Hour of Web Surfing

| | Using No Security Systems | Using Standard Security Systems | Using Secure-Surfer |
|-----------------------|---------------------------|---------------------------------|---------------------|
| Standard Sites | 17 | 3 | 0 |
| Bad Sites | 96 | 32 | 0 |

Secure-Surfer, LLC Test

In this context, a 2006 *eWeek* study found that 92% of all PCs were infected with an average of seven pieces of adware, spyware, and other types of malware. Moreover, a large portion of this malware is reportedly stealing passwords and logging keystrokes with the intent of profiting from identity theft. According to The Anti-Phishing Working Group, the number of unique password-stealing malwares disseminated through the internet during the past year has oscillated between 180 and 345 a month (see chart below).⁶

Password Stealing Malicious Code. Unique Applications



Secure-Surfers™ are a fail-safe, easy to use, and inexpensive means for eliminating the shortcomings of today's solutions for protecting internet web browsing communications. In particular, **Secure-Surfers™** provide total protection against the loss of credentials and privacy even when these communications are conducted from untrustworthy PCs. In addition, **Secure-Surfers™** provide a web-browsing environment that eliminates the possibility of downloading malware and protects users from existing malware infections in their PCs. Figure 1 below illustrates how **Secure-Surfers™** connect to the internet. The built-in web browser application in the Secure-Surfer™ is only able to access internet sites after passing through authentication controlled by Secure-Surfer, LLC's NarrowGateKeeper (NGK) authentication server.

⁶ Phishing Activity Trends: Report for the Month of January 2007, Anti-Phishing Working Group.



Figure 1. Using the Secure-Surfer™ Key to Access Internet through SECURE-SURFER, LLC's NGK Server

2. Secure-Surfer™ Architecture

The security enhancements of Secure-Surfers™ come from three techniques: a write-protected web browser application software that resists malware infections, a controlled secure write that updates the web browser application when necessary, and an anti-replication authentication that resists attackers from stealing user credentials.⁷ Secure-Surfers™ build these three techniques into a specially customized USB device to enhance internet web browser access security. The memory storage of the USB device is divided into multiple regions, each with different read and write (I/O) properties. The security enhancements come from the following facts related to these memory regions:

- A bootable and write protected region containing an embedded operating system that can interact with the PC's BIOS and boot to a native operating system mode. It can also run as a virtual machine within a host MS Windows™ operating system if not booted from BIOS.
- A selective write-protected memory region that holds a Firefox web browser. The region is not writable when the USB device is directly used as a storage peripheral of a host operating system, but is writable by the USB device's embedded operating system. By making it write-protected, the built-in application, such as the browser, would not be infected by malicious plug-ins.

A write-protected and read-constrained region that holds the authentication credential (a piece of data that is shared between the server and the client). The memory region provides fast read responses for sparse read requests over time, but slow responses for consecutive read requests. Contact Secure-Surfer, LLC for further details on this technology.

5. SecureSurfer™ Applications

Remote & Mobile Corporate Network Users: Many organizations need to provide access to their internal private networks to remote employees, partners and suppliers. The preferred means for accessing these networks is through the internet using PC web browsers. However,

⁷ These techniques are included in Secure-Surfer's NarrowGate™ Appliance technique [patent-pending #60/730,239, October 25, 2006] and NarrowGate™ Authentication technique [patent-pending #60/828,148, October 4, 2007].



these PCs are potentially infected with malware that is designed to steal user credentials and company secrets and that is able to spread into the corporate network and other PCs connected to this network.

To protect against this, some companies pre-configure each user's PC for remote access and scan these PCs for malware infections every time they request network access. Unfortunately, this pre-configuring is expensive and cumbersome to administer and malware scanning still leaves some malware undetected. Moreover, this approach restricts users' choice of devices for logging on to the network to company-issued and pre-configured PCs. Thus, for example, executives requiring access to the network while traveling can be left stranded without critical network access in the event of losing their "pre-configured" company PC laptops. With **Secure-Surfers™** these mobile workers can securely access the network from colleagues' PCs, public PCs in hotel lobbies, or ANY other available PC.

Networks that limit remote access to PCs equipped with **Secure-Surfers™** eliminate the threat of hackers stealing user credentials and logging on to the network with these stolen credentials. Also, they can protect the network from malware resident in users' PCs. User credentials cannot be stolen, even when access takes place from an untrustworthy PC. Since each **Secure-Surfer™** key is unique and issued to an individual, access can also be monitored for auditing and regulatory compliance (e.g., The Health Insurance Portability And Accountability Act Of 1996 (HIPAA) and The Sarbanes-Oxley Financial And Accounting Disclosure Information Act of 2002 (SO)).

Secure-Surfers™ provide this level of protection to mobile and remote users even when these are using wireless (WiFi) communications and non-SSL protected connections. Most of the local area network traffic within organizations such as enterprises and universities are not conducted using SSL. However, these organizations increasingly need to provide users with internet access through wireless (WiFi) networks that are more vulnerable than wired networks. Indeed, attackers can easily launch traffic sniffing from anywhere that can pickup a wireless signal (e.g., in the parking lot of a business). It is also easier for attackers to build a spoofed route or DNS service for connection hijacking and identity phishing and such attacks are increasingly common.⁸ The state-of-art protection practice for WiFi networks is WAP, which provides limited encryption protection to the wireless network traffic and is easy to break. As a result of these vulnerabilities, non-sophisticated WiFi users are at a significant risk of being tricked by attackers through phishing and hijacking. This fact makes the WiFi network very unsuitable to carry traffic for serious business.

Secure-Surfer™ enables a safer WiFi network experience by providing authentication and routing through the NarrowGateKeeper proxy service. First, only authenticated users employing **Secure-Surfers™** can access the NarrowGateKeeper server. The authentication mechanism is built into the **Secure-Surfer** device, which automatically launches authentication negotiation with NarrowGateKeeper server. The authentication is mutual for both server and client to ensure the client only communicates through SECURE-SURFER, LLC's NarrowGateKeeper server and the server only permits trustworthy SECURE-SURFER, LLC users to use the services.

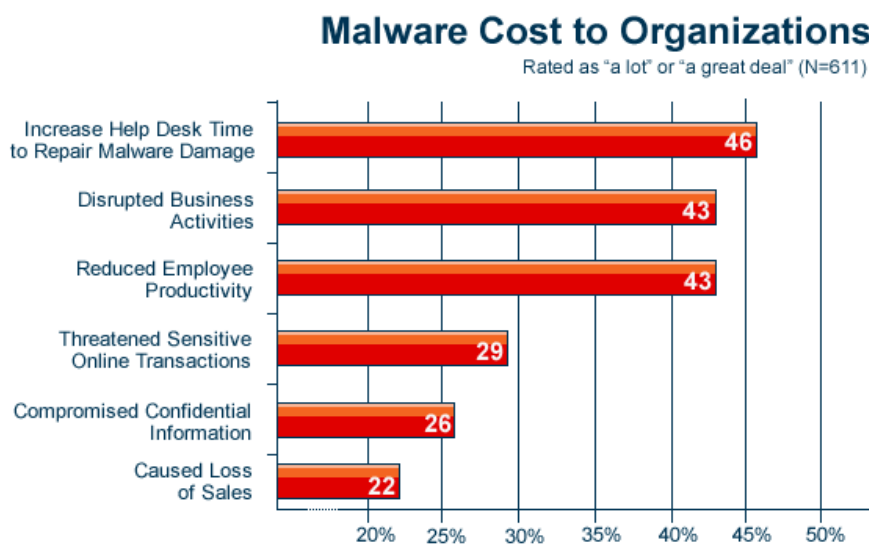
⁸ See for example, [Malicious Website / Malicious Code: Crimeware, Trojan Horse Bot](#), WebSense Security Labs Alerts, Feb. 21, 2007, and Ryan Naraine, [Trojan Redirector Ups the Ante in Online Banking Attacks](#), e-Week.com, March 21, 2006.



After the mutual authentication, all the Secure-Surfer's™ internet accesses have to relay through the NarrowGateKeeper, which acts as an internet network proxy. The proxy differs from a regular proxy by the fact that its traffic between Secure-Surfer™ browser and NarrowGateKeeper server is all delivered through a secure SSL tunnel that is built after the authentication. In this way, the traffic is immune to traffic sniffing attacks launched between client and NarrowGateKeeper. The client's Secure-Surfer™ only recognizes and connects to the designated NarrowGateKeeper server, which is hard coded into the Secure-Surfer™ device. The client Secure-Surfer™ does not make any local name resolution for any other destination servers. In this way, it is completely immune to DNS hijacking and phishing attacks against the client side. By protecting against these two common problems (sniffing and hijacking), Secure-Surfer's™ provide authenticated and private web surfing even for users connecting through WiFi networks and non-SSL enabled connections.

Web Server Customer Service Costs Containment: Providing customer support for a large group of users is always challenging. This is particularly difficult for Internet-based services such as online banking because of the large variety of reasons that could deny users from accessing offered services. Worse yet, these reasons are often not directly related to the offered service. For example, failure of an ISP, client operating system, or an infected client browser could all deny legitimate users from accessing his/her account even when the server side software is in perfect condition and being used by many other customers.

Because malicious software is widespread and PC's architecture open, these problems are so common that many support efforts of network services are spent in the diagnostic and recovery of end user's browser software, network configuration, and operating system, even though these have no direct relationship to the network service being offered. The table below suggests that malware infections have a profound impact on organizations' customer service costs.



Source: Webroot Software, Enterprise Market Research Study, January 2207



Although most of network services offer detailed online trouble-shooting and self-diagnostic procedures, users often fail to access these procedures because their browsers or network configurations are malfunctioning. In some cases, the supporting team ends up making a reinstallation of the operating system simply to get a working browser to access additional troubleshooting information on the Internet. The table below illustrates the average cost of help desk, reinstallation, and loss of productivity for an organization supporting 14,000 workstations.

| Malware Cost Analysis: Company X with 14,000 Workstations | | | | |
|---|---|---------------------------------------|------------------|------------------|
| Help Desk Costs | | | | |
| Average percent of users with a malware-related call each month | Average number of malware-related calls per month | Average cost per call | Monthly Cost | Annual Cost |
| 7.5% | 1,050 | \$20 | \$21,000 | \$252,000 |
| IT Support Costs for Machine Re-Imaging | | | | |
| Average number of machines re-Imaged per day | Average hours needed for each re-Image | Average hourly rate for employee time | Monthly Cost | Annual Cost |
| 3 | 3 | \$50 | \$9,000 | \$108,000 |
| Lost Productivity of Employee (user) with Affected Machine | | | | |
| Average number of employees with affected machines per day | Average hours of lost productivity while machine is being re-Imaged | Average hourly rate for employee time | Monthly Cost | Annual Cost |
| 3 | 3 | \$50 | \$9,000 | \$108,000 |
| Total Costs: | | | Per Month | Per Year |
| | | | \$39,000 | \$468,000 |
| <i>Source: Webroot Software Threat Research Department</i> | | | | |

The use of **Secure-Surfers™** for internet browsing can significantly reduce these customer service costs, particularly because browsing is by far the major source of PC malware infections. **Secure-Surfer's™** browsing eliminates incidences of downloading malware into users' PCs and provides trustworthy and reliable internet access, even when the host PC is infected with malware.

Financial Service Providers: Financial institutions are the target of over 80% of malicious activity on the internet and increasingly subject to regulations requiring better means for ensuring the identity of online users. Indeed, in many countries only users equipped with an authentication device such as a **Secure-Surfer™** are permitted to conduct online banking. **Secure-Surfer's™** cost per customer is so inexpensive that a bank could offer the **Secure-Surfer™** keys and service as marketing give-away to (1) significantly reduce the risk of online fraud; (2) realize significant savings by encouraging more customers to employ on-line banking services, which are about 10 times less expensive to deliver than "brick and mortar" services;⁹ (3) attractively differentiate its enterprise; and (4) better comply with regulations such as the U.S. Federal Financial Institutions Examination Council (FFIEC) "Authentication in an Internet Banking Environment Regulation".¹⁰

⁹ Stronger security measures would reportedly encourage 31 million persons in the United States to start banking online, 39 million more to increase their online banking usage and raise annual banking industry profits by \$8.3 billion (see: Tricipher Consumer Online Banking Study, Javelin Strategy Group, March 2007).

¹⁰ Federal Financial Institutions Examination Council "Authentication in an Internet Banking Environment", www.ffiec.gov.



In the United States, stronger security measures would reportedly double online banking usage, raising banking industry profits by \$8.3 billion.¹¹ Indeed, 74% of Americans do not believe that current practices for identifying themselves online to their banks and other eCommerce services are safe and most are willing to adopt stronger security methods to log on, including token-based solutions such as **Secure-Surfer**^{TM,12}. Over the next decade, about 40% of the world's population will use banks for the first time ever. The adoption rate of these banking consumers will depend critically on convincing them that online banking and e-Commerce are safe.¹³ **Secure-Surfer**TM is a compelling and unmatched approach to providing this safety with ease of use and low cost.

Banks and eCommerce suppliers provide online security to their online retail customers with simple software solutions, while providing their business customers with stronger authentication devices such as smart cards, one-time passwords, and biometric identification devices.¹⁴ **Secure-Surfer**TM is significantly superior to all of these solutions because it works reliably even when users communicate from untrustworthy PCs and networks and is comparatively easier to use and less expensive.

Individuals: Managing PCs for accessing the internet securely can be daunting. Software for identifying and eliminating malware requires continuous updating and web surfing inconveniences users with a myriad of prompts to accept or reject operations that can potentially harm their PCs and compromise their privacy. Most users lack the time and understanding to keep up with these prompts and updates. As a result, these users' PCs typically become highly prone to malware attacks, freezes and slowdowns associated with poor software maintenance.

Secure-SurfersTM relieve users from having to conduct or worry about such maintenance, providing robust appliance-like web access, even from PCs infected with malicious malware. This is particularly important in those occasions when users have an urgent need to access information on the internet, but their PC browser is not performing properly because its code has become corrupted or the PC is infected with malware. **Secure-Surfers**TM also protect against snoopers recoding or seeing these users' internet activity. This is particularly important when the cost of losing privacy while surfing the internet is high (e.g., when entering personal passwords or credit card or other security information that could be used to illicitly access these users' financial assets or records). Of course, **Secure-Surfers**TM are also useful to these users when the risk of downloading malware from the internet is high.

Healthcare: Medical records are increasingly stored and available in digital formats and patients, insurance carriers, doctors, and employers need secure access to these records using their PCs' web browser. Regulations such as HIPAA require that organizations storing and transmitting these records ensure that these records are only viewed by those authorized to do so. However, as discussed earlier, credentials for accessing these records remotely using a standard web browser from a PC are easily stolen by malware. This vulnerability is particularly

¹¹ Tricipher Consumer Online Banking Study, Javelin Strategy Group, March 2007.

¹² National Cyber Security Alliance and Bank Of America, "Online Fraud Report." <http://www.staysafeonline.info/>. May 2006. 1 Nov. 2007 <<http://www.staysafeonline.info/news/onlinefraudreportfinal.pdf>>.

¹³ James Greene, *Bank Technology News*, May 2007.

¹⁴ Federal Financial Institutions Examination Council "Authentication in an Internet Banking Environment", www.ffiec.gov.



strong for PCs that are not tightly supervised by network operators, such as those of patients or doctors. **Secure-Surfers™** provide an inexpensive and fail-safe means for providing the needed protection to comply with regulations and ensure privacy.

In addition to increasing the survivability of web browsing in untrustworthy environments, **Secure-Surfers™** can also be used to make online access more accountable. A server often wants to ensure that its service is only available to authorized users and that users cannot share the service with others without the server's permission. Currently, users of SSL-style of authentication can violate this without being detected by the server. Users can offer anyone copies of the authentication credential and thus ability to access the service. Since **Secure-Surfers™** are not replicable and each is unique to its user, network operators can constrain network access to users who physically possess a **Secure-Surfer™**. This functionality is also useful for many applications especially those requiring strong digital right management (DRM) to protect rights of media creators and distributors and to comply with regulations such as HIPAA and SO.

6. Conclusion

Protection against online internet fraud requires a combination of authentication and privacy to ensure end-to-end secure communications, and the detection of malwares and the defense against them. The principal means for achieving the first of these are mechanisms such as SSL that provide server authentication, client authentication, and an encrypted connection but presuppose that the client PCs of communicating parties are trustworthy. **Secure-Surfers™** ensure that SSL provides protection even when communications take place from untrustworthy client PCs.

The current state-of-the-art means for ensuring that PCs are trustworthy (free of malware) are based on *signature* or *fingerprint* filtering of known malware. Although recent malware detection and prevention techniques have improved significantly and have succeeded in protecting against many malware attacks, the approach is nowhere close to eliminating all malware. Moreover, a user could possibly protect his or her own PC but this would not help when needing to use an untrustworthy PC, such as during travel time. **Secure-Surfers™**, on the other hand, address the challenge in an untrustworthy environment. Rather than setting the goal to be completely malware free to ensure secure online access, **Secure-Surfers™** are a mechanism to increase survivability for online access in malicious environments. This approach is orthogonal to the current signature-based malware filtering and detection techniques and can be combined with these techniques for better security.