



Keystroke Encryption Technology Explained

Updated February 9, 2008

information@bluegemsecurity.com

(800) 650-3670

www.bluegemsecurity.com

Executive Summary

BlueGem Security is introducing keystroke encryption technology, patented transaction security software into North America and Europe. It effectively blocks all spyware, Trojan horse and keylogger threats by utilizing a two pronged approach. It uses both 128 bit encryption technology to encrypt every user keystroke and because the technology resides in a layer between hardware and the operating system, also bypasses the operating system where these threats exist. It then delivers each keystroke directly to the user's secured web browser or designated application. This preventative solution is very different from existing anti-spyware and anti-keylogger solutions. BlueGem's Keystroke Encryption has a very small footprint which can be quickly and simply deployed and it links to websites and pages that are pre-specified by each customer. The software can best be leveraged on high security web pages known as 'HTTPS'. When used in conjunction with Secure Socket Layer (SSL) or HTTPS, high security encrypted websites, BlueGem's Keystroke Encryption solution effectively creates an end-to-end tunnel of encrypted information from the user's keyboard to the secure server; thereby safely delivering the user's information and eliminating any chance of it being intercepted by Spyware. Typical applications are internet banking, online PC games, credit cards, insurance and securities trading, Government agencies and VPN access, due to its proven security and cost effectiveness over two-factor token technology.

The security gap that exists today is in the end-user's computer. Secure Socket Layer (SSL) or HTTPS only encrypts traffic traveling over the internet network and does nothing to protect identity theft on the PC itself. Web browser encryption technology was developed in 1998 when hacking was perceived to be at the network level. When utilizing an Internet portal however, the security gap on the end-user's PC can be exploited by identity thieves through various hacking methods such as spyware and Trojan horses. These constantly evolving threats are used to steal users' passwords, login names, and other confidential information.

Threats and hacking methods are targeted at end-user computers and research confirms the severity of such vulnerability:

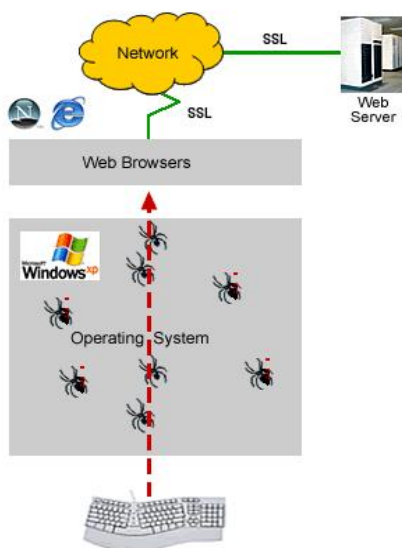
- Identity theft caused by spyware and especially keyloggers, accounted for 11.6% of total identity theft, which translated to over \$3.1 billion dollars in 2004. - BBB survey conducted amongst 4000 consumers.
- 67% of PCs are infected with spyware, which can steal personal information and facilitate identity theft. - IDC Report.
- 20% of Americans have already experienced identity theft, with financial institutions facing growing pressure to prove how they combat fraud. - Unisys Corporation research report.
- Concerns about identity theft are beginning to put people off shopping and banking online, with 17% of people saying they had stopped banking online while 13% had abandoned Web shopping. - Survey commissioned by software firm Intervoice in the UK.

The Problem

Gartner Research states: “Online customers want strong security measures that go well beyond passwords. The two factor authentication methods of One-time password tokens and Public Key Infrastructure using digital certificates or soft certificates are not practical and very expensive.” In a separate report, Gartner states: “U.S. banks are reluctant to, but should adopt stronger customer authentication”. A Gartner survey reveals a surge in unauthorized transfers from checking accounts and credit card accounts over the past year. Further, according to an RSA Security survey, 25% of Internet shoppers reduced their internet purchases due to security fears. Clearly consumers today are still very concerned about the security of the internet and are often reluctant to provide any sort of personal information online. Banks and credit card companies, security companies, companies with VPNs and the many companies that need to transmit secure keyboard entered data must implement ways to protect against spyware. This is necessary not only to maintain the confidence of their existing customer base, but also to win over skeptical public confidence and grow their online businesses.

The Threat

With consumers increasingly wanting to access accounts from anywhere, at anytime; providing the peace of mind needed to maintain consumer confidence is becoming increasingly difficult. Ever larger numbers of keyloggers, Trojan horses, other spyware and viruses are bombarding online portals, which is limiting and in some cases reducing consumer adoption of online services. Keyboard loggers are able to infiltrate individual PCs with relative ease, gaining access using many ingenious and rapidly evolving methods, often undetected by anti-virus and anti-spyware products which, by virtue of the way they are designed, are always in a catch up mode. This type of spyware can record everything that consumers type, including usernames, passwords, Social Security, bank account and credit card numbers. This is due to the way in which web browsers are designed to operate. Many other types of sensitive information from medical records to confidential family information is also vulnerable to the prying eyes of keystroke loggers. Often this information is very selectively collected. Recent keylogging programs have been discovered, which only collect the information that is entered via keystrokes for specific URLs such as sign-in pages for financial institutions, which significantly escalates the risk of online fraud.



Malicious software that is secretly installed on PCs can record the keystrokes used to enter user IDs and passwords for accessing online bank and other confidential accounts. Keylogging software can be installed locally by cyberthieves (such as on a computer at a cybercafe or university computer room), or by viruses and worms that install the software over the Internet. Malicious software often arrives as a Trojan horse which can easily be attached to a legitimate website, looks like a legitimate application and eavesdrops on user actions.

Financial institutions or online game providers can minimize problems from keyboard logging by preventing connections from unknown machines. However, this is often an impractical and inconvenient measure that eliminates the convenience of accessing online services from anywhere, at anytime.

What are Keyloggers and what is next?

A keylogger – also known as, key logger, or keystroke logger - is a program that runs in the background, recording a user’s keystrokes. Typical spyware programs use multiple tactics to steal a user’s identity information and keystroke logging is the major and most effective threat to the loss of a user’s identity. Once keystrokes are logged, they are hidden in the machine for later retrieval, or shipped directly to the attacker, often through a back door port in the computer and undetected by firewalls and anti-spyware programs. The current trend of spyware attacks on users’ identities suggests that they will continue to increase and become ever more sophisticated and stealthy¹. BlueGem analysis shows that malware is becoming more intelligent and we expect to see Artificial Intelligence based malware in the future. The table below describes the evolution of discovered keyloggers over time.

Generation	Features	Observed Trend	Examples
First Generation	Hacking code	Manual hacking to a selected user’s computer or a groups computers	IK97, Back Orifice, School Bus, Serve 7, etc.
Second Generation	Combination of virus and Malware	Upon infection of virus, it automatically executes a malicious hacking code	VBS/Love_Letter, Win-Trojan/Sneaker, Win-Trojan/Secokys, Win32/Badtrans.worm.29020, etc.
Third Generation	Self-defense enabled	Ability to terminate/disable anti-virus & anti-spyware and personal firewall programs	Bugbear, Anti-Spyware Killer, Rootkits, etc.
Fourth Generation	Self-evolutionary and completely stealthy	Artificial Intelligent (AI) and self-diagnostic ability and stealth	Blue Pill, Detect_this_Keylogger.msi, etc.

What Are The Shortcomings Of Current Tools?

Antivirus or current Internet Security Suites that rely on scanning technology look for malicious programs, files or processes, such as keyboard loggers, by using signature-based software.

Signature-based scanning programs

Signature-based programs include standard anti-virus and anti-spyware scanning software. The limitation of this approach with regard to detection of keystroke loggers is that the anti-virus and anti-spyware software is only as good as the last update and scan on the user’s PC. Even with complete vigilance and daily scans, users are completely dependent on their vendor’s ability to keep up with the latest rapidly evolving security threats. It has been estimated that the time it takes a vendor to develop a new virus vaccine and patch ranges anywhere from two weeks to even months in the case of highly

¹ BluePill is a primary example of stealthy malware that can not be detected by antivirus programs.

targeted malware. This gap is typically referred as Zero day vulnerability. However, when spyware targets a specific individual or an organization – this method is widely used in the intelligence community and by organized crime groups – signature based solutions become ineffective, because anti-virus/spyware vendors deal with massively distributed malicious codes which target the general public on an indiscriminate basis. According to a recent report, increasingly organized offshore criminal groups are developing new super smart spyware.

Anti-spyware software solutions generally work better than regular anti-virus solutions when it comes to detecting malware. However, anti-spyware solutions are generally signature based and a signature base solution has three major vulnerabilities; 1) It requires frequent updates to maintain an up-to-date signature database, 2) Even ‘up-to-date’ signature databases do not cover unknown or registered commercial key loggers, 3) It consumes significant PC resources to constantly run scan files and to monitor processes.

Personal Firewall

A personal firewall is software that acts as network traffic security and which is installed on an end-user's PC. It controls communications to and from the user's PC, permitting or denying communications based on the selected Security Policy. A personal firewall provides some level of intrusion detection, allowing the software to terminate or block connectivity where it suspects an intrusion is being attempted, but at the same time, personal firewalls can easily be compromised by advanced malware that can terminate or manipulate the software.

Problems and weaknesses

Personal Firewalls are installed on the system they are designed to protect, and malware attacks on the firewall can also affect that system and vice versa:

- Instead of reducing the number of network-aware applications, a personal firewall is an additional service that consumes system resources and can also be the target of an attack, as the Worm Witty has already shown.
- If the system has been compromised by malware, spyware or similar software, these programs can also manipulate the firewall, because both are running on the same system. In the past, security experts have found numerous ways to bypass or even completely shut down software firewalls as well as the discovery of new spyware that can terminate the MS anti-spyware program.
- They will often alert the user about attacks on harmless occasions, for example connection attempts to closed ports, or can misinterpret normal network traffic as an attack.
- Firewalls can't detect Trojan horses that are used for keystroke logging because Trojan horses look like normal, "friendly" programs. They are also 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.

How about Password Manager

Password Managers are often misconstrued as major security tools. In fact, Password Managers are convenience tools which assist users by memorizing the passwords used on numerous websites. Although the tool will help to increase the user's level of password security, these password managers include the following vulnerabilities (1) when users register their password information, their identity information can be captured by spyware; (2) when password managers submit the user password to web

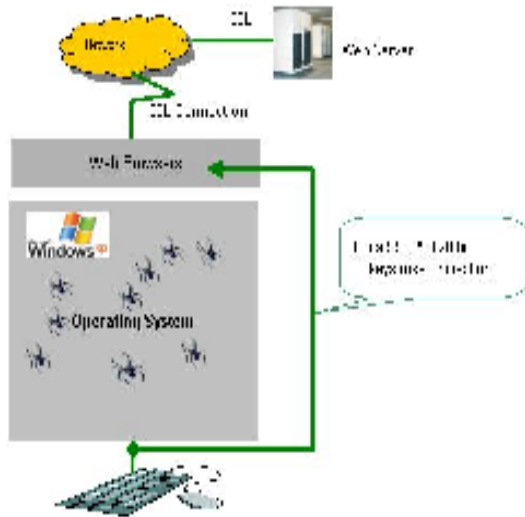
pages, the password still can be intercepted by browser based malware, known as Man-in-the-Browser attacks.

Keystroke Encryption technology – a key protection in transaction security

BlueGem Security Keystroke Encryption software blocks malware that uses keystroke logging technique, which is a predominant way of hacking, to steal user transactions. It does this by employing a dual protection approach which uses a 128 bit encryption algorithm to encrypt every single user keystroke and also bypasses the conventional keystroke delivery channel in the Operating System where threats reside. In other words, BlueGem Security software creates a virtual ‘encryption’ channel right from the keyboard and delivers the user data directly to the web browser:

- BlueGem Security solution encrypts each and every keystroke at the lowest layer where software can reside; which means that no malware can go under the layer where BlueGem Security encrypts the user’s data.
- BlueGem Security Keystroke Encryption solution has multiple layers of protection to prevent the possibility of malware attacks that may attempt to disable any of BlueGems’ modules.
- Every user keystroke is encrypted on a character-by-character basis, and each individual keystroke is encrypted with an independent encryption key. The benefit of this encryption method is that it adds extra security to the user’s information by using a separate encryption key for every keystroke. For instance, even if a hacker cracks an encrypted character, he could only understand one single character instead of an entire stream of data (Keystroke Encryption).
- Once a keystroke is encrypted, it is routed through a virtual channel and decrypted at the hand-off point in the browser where it initiates a Secure Socket Layer connection to the web server (Virtualization of Data Input).
- BlueGem Security automatically activates its encryption channel when it recognizes a valid client’s web domain, and then fully extends an encryption channel to the user’s keyboard. This method not only enables SaaS based online security protection, but also gives a significant marketing advantage to our clients who view security as a major marketing differentiator.

The following diagram illustrates how, when BlueGem Security Keystroke Encryption is operating, malicious programs and Trojan horses cannot see the encrypted keystrokes because data entered uses 128 bit encryption and is delivered to the application queue through a separate, discreet channel.



1. BlueGem encrypts every single keystroke using 128 bit encryption and delivers the encrypted keystrokes directly to the web browser while bypassing the conventional keystroke delivery channel in the OS.
2. BlueGem encryption driver resides at the Kernel level in the OS, beyond the reach of today's malware (patented method).
3. BlueGem driver is protected from hacking attacks by multiple redundant integrity checking mechanisms (patented method).
4. BlueGem operates with Windows 98, through Vista and supports IE 5.0 and above and the latest FireFox browsers.

Applications for BlueGem's Keystroke Encryption Technology

Examples of typical applications for this software are:

- Login ID and Password pages for Internet banking and stock trading account access.
- Access to Corporate portals and web pages that require high security from Spyware.
- VPN Access.
- Online credit card, mortgage and loan applications, where protection of a user's credentials from spyware is critical.
- Health Care and Life Sciences compliance with HIPAA requirements.
- OEM – Integrating BlueGem's technology into your offering will insure your customers the highest degree of protection of their confidential information.
- Any web pages that require high security from spyware threats.

Systems Requirements

- OS: Microsoft Windows 98, 2000, XP, Vista 32 and 64 bit
- Browsers: Internet Explorer 5.0 and above, Firefox 2.0 and above
- CPU: Pentium II and above and AMD K5 above
- Memory: 64 M Bytes or greater