



White Paper

## Software Security Token™ (SST)

Charles Manick Livermore  
December 3<sup>rd</sup>, 2004

### Introduction

Strong two-factor user authentication has proven to be the only successful method to prevent unauthorized access to critical networks and machines. Strong user authentication is more secure than static passwords, as it relies upon something the user knows (such as a pass-phrase) and something they possess such as the Software Security Token (SST). SST controls access to systems or networks through the use of a challenge-response system, creating an encrypted, unique identifier each time access is attempted.

Outdated methods to secure connections to sensitive web sites, such as username / password pairings have failed. Attempts to enhance password security with methods such as SSL encrypted connections are unsuccessful. These methods fail due to password sniffing programs, Trojan horses, social engineering scams (phishing) and other methods.

Phishing schemes and Trojan horses cost businesses millions of dollars. TowerGroup analyst George Tubin says this will result in, " the potential loss of customer confidence in the Internet, not to mention loss of trust in financial institutions themselves."

Until now secure authentication has required the user to carry a small hardware token to calculate the response to a server challenge for authentication. These tokens are so expensive that they are not practical for use by online banking and other customers. The SST software solution is less than one-tenth the cost of hardware tokens and easy to use.

### Passphrase Protection

Every user of SST has a unique passphrase that is used to unlock the SST program. A passphrase differs from a password in both length and complexity. Passphrases can contain nearly any character string including spaces and numbers. As passphrases can be of variable length and are case-sensitive they are almost impossible for an unauthorized user to guess correctly. Passphrases are also more user-friendly, as instead of having to remember a random series of letters and numbers, they can choose some phrase they will remember.

### Challenge-Response Authentication

SST authenticates access through the use of a challenge-response method. When a user establishes a connection to a secured system or network, they first enter their user name and then are prompted by the challenge, an 8-digit random number. This number changes every time a new challenge is generated.

This user must then enter this challenge into SST, which then supplies the correct 8-character hexadecimal response. The user then replies to the challenge with this response and is granted access.

The challenge-response architecture utilized in SST provides an unprecedented level of security for a system or network. Without the proper response to a challenge there is only one chance in 4.27 billion for someone to guess the correct response. If an unauthorized user tried to guess the valid response and kept trying every 5 seconds, it would take on average more than 320 years to guess the correct response.

### **The cost of insecure authentication**

Social engineering attacks have proven to be among the most effective ways to gain access to secure systems. Legitimate looking emails and fraudulent websites deceive and exploit users into revealing sensitive information. According to a Gartner study more than 1.2 billion dollars were lost by banks and credit card companies last year due to identity theft caused by phishing attacks.

### **Added webserver security**

For protecting web servers, SST interfaces with Webgate Plus. Webgate Plus with SST provides strong user authentication to a web server, ensuring that not only is the web server protected from network and application level attacks, but that only legitimate users are granted access to the web server. Webgate Plus is an in-line solution that sits between the client computer and the protected web server. More information on Webgate Plus is available on our web site.

For more information contact us at:

Livermore Software Laboratories, Intl.  
Division of Fremont Avenue Software, Inc.  
1830 S. Kirkwood Suite 205  
Houston, TX 77077  
Phone: 281-759-3274  
Fax: 281-759-8558  
e-mail: [portus@lsli.com](mailto:portus@lsli.com)  
Web: [www.lsli.com](http://www.lsli.com)

### **Features of SST**

- ▶ **Passphrase protection:** more secure than passwords or PIN numbers.
- ▶ **Encryption:** SST utilizes a unique encrypted keyfile for each user.
- ▶ **Challenge-Response Architecture:** provides the highest levels of secure authentication.

### **Low cost per user**

SST is an extremely affordable solution, costing far less per user than a comparable hardware security token solution.

### **Ease of use**

SST runs on Windows for end users, and on AIX, Linux and Solaris for the host servers. A java SST client is also available. The convenience of use and low cost to implement guarantee user acceptance. The SST client package consists of three files: the SST program itself, its configuration file, and the encrypted keyfile.