Harden SSL/TLS v1.01

Windows hardening tool

Thierry ZOLLER

http://blog.zoller.lu
http://www.g-sec.lu

G-SEC™ is a non-commercial and independent group of Information Security Specialists based in Luxembourg. Our work has been featured in New York Times, eWeek, ct', SAT1, Washington Post and at conferences ranging from Hack.lu to Cansecwest.

Table of Contents

Introduction

"Harden SSL/TLS" allows to configure and harden the SSL/TLS settings of Windows XP to Windows 8 and from Windows 2003 to Windows Server 2012.

Harden TLS allows to remotely set SSL policies allowing or denying certain ciphers/hashes or complete cipher suites.

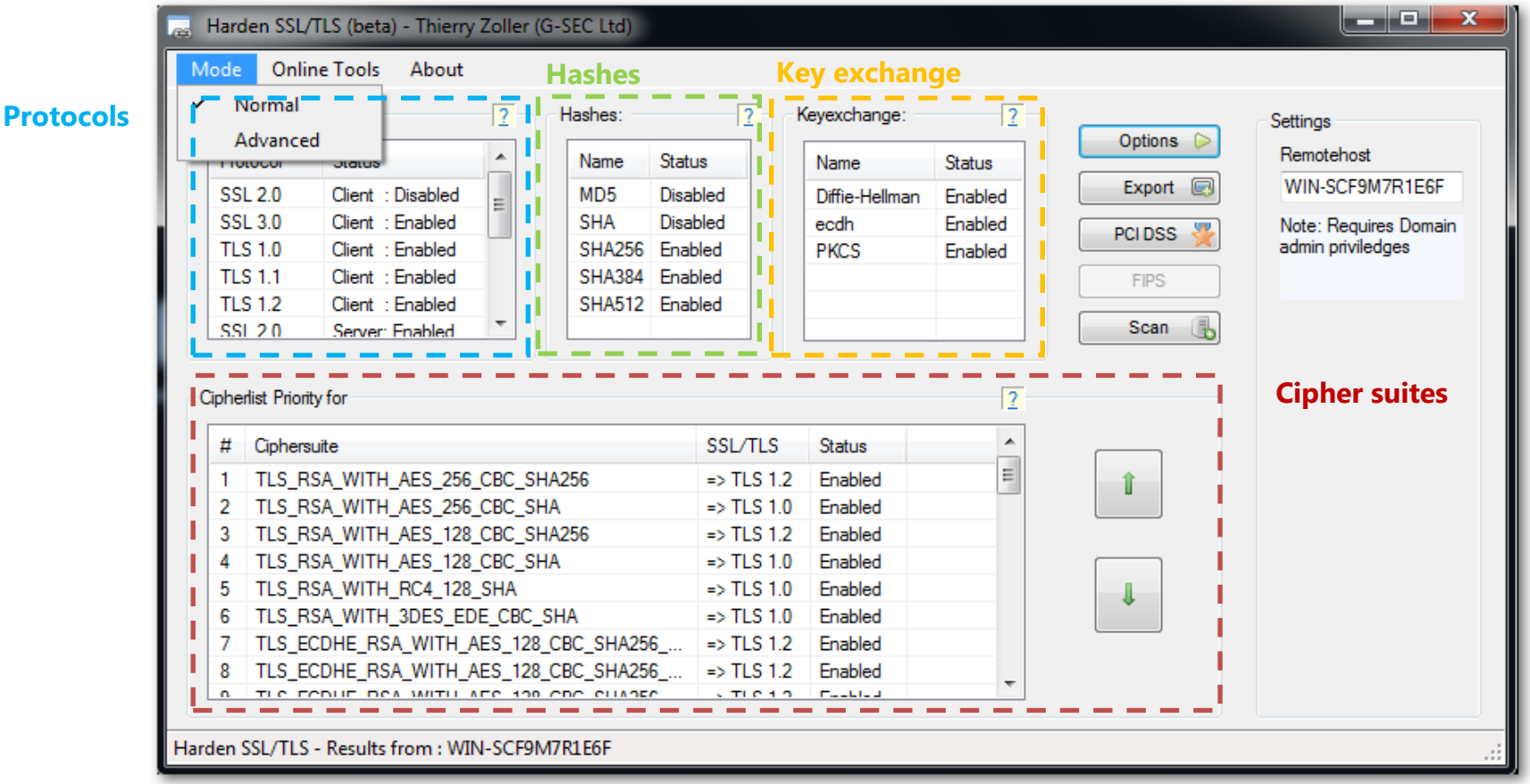
The foundation of this tool was the investigation and reverse engineering of the ciphers provided by the various SCHANNEL versions by G-SEC and presented in the paper "SSL/TLS Compatibility Report 2011".

This tool specific allows setting policies with regards to what ciphers and protocols are available to applications that use SCHANNEL crypto interface. A lot of windows applications do use this interface, for instance Google Chrome as well as Apple Safari are a few of these. By changing the settings you can indirectly control what ciphers these applications are allowed to use.

This tool works on all and every application that uses SCHANNEL whether they are client or server applications - as example: IIS, SQL Server, Internet Explorer, Safari and a lot of others.

Usage

- Options : Allows to enter the name of a remote Machine
- Mode : Allows to choose from Normal or Advance mode – The advanced mode is documented in the section “Advanced Mode”
- Export : Export/Backup all affected registry keys
- PCI-DSS : Adjust the settings as to comply with PCI-DSS
- Scan : Scans the host entered in “Settings – Remote host”



Protocols

The protocol table shows the Protocols enabled or disabled on a Server/Client logic, to enable a protocol simply double click on the item you want enabled. Note: For Vista and up “Harden SSL/TLS” also automatically configures Windows Internet Settings with the correct settings.

Note: Windows 7 and Windows 2008R2 come with TLS1.2 disabled by default, to enable it for IIS 7.5 just double click on the appropriate TLS 1.2 entry.

Hashes

List currently available hashes

Key exchange

List the currently available key exchange algorithms

Cipher list

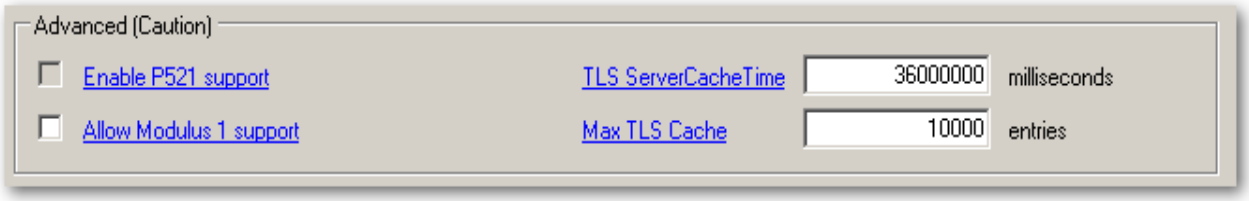
The display and function of this list changes depending on the OS version.

- **Windows 2000, XP, Server 2003**
  The list allows you to enable/disable ciphers; if you disable an cipher it will not be available to the applications even if they request it.

- **Windows Vista/7/8, Server 2008/R2, Server 2012**
  The list allows you to enable/disabled and prioritizes cipher suites. The first item displayed is the preferred cipher for an SCHANNEL client or server, you can change this cipher to (as example AES 256) by pushing the UP and DOWN buttons, Harden SSL/TLS will keep a state map of which ciphers are, enabled, disabled and the their past and present order.

Advanced Mode

The advanced mode allows access to more advanced settings



- **P521 mode**
  Microsoft removed default ECC P521 support after Vista and Server 2008, this options allows to re-enable and re-introduce ECC P521 mode for Windows7, Windows 8 and Windows Server 2012

- **Modulus 1 support (You probably do not want to enable this setting)**
  When a Web server uses a certificate with an RSA public key exponent of 1, the private key exponent is also set to 1. If these conditions are present, the connection has no encryption security. Enabling this will configure your client/server to allow a connection to a Web server that uses a certificate with an RSA public key exponent of 1.

- **TLS/SSL Cache time out**
  One reason for changing the default value for the SSL session cache is to force the client to authenticate more often. More frequent caching is sometimes useful, for example, if you want to reduce the computational effort (performance) or if you know that the client is using a smart card and you want the Web page to be accessible only when the user inserts the smart card in the reader.

  Before changing the SSL cache time-out interval, make sure that HTTP Keep-Alives are enabled (HTTP Keep-Alives are enabled by default).

No secure session caching	0 (turns off session caching)
2 minutes (Windows NT 4)	120000
5 minutes (Windows 2000)	300000
10 hours (2000 SP2, XP, 2003,2008, 2008R2)	36000000

- **TLS/SSL Cache size**

  IIS maintains objects in memory to track each incoming Web connection. After five minutes of idle time, these objects are destroyed to reclaim resources. During this process, IIS purges the SSL/TLS session ID that the operating system caches from the session ID cache table. IIS also purges all the connection information that is negotiated between the client and the server. When a client tries to resume an SSL/TLS session by using the previous session ID, the server cannot locate the connection information in the cache. Therefore, the client must renegotiate the connection. Additionally, the client must obtain a new session ID. **Increasing the cache size may reduce the cpu load but increases memory usage, each session cache element typically requires 2-4k bytes of memory**

Default	10.000 entries

Known limitations

- Initializes and sets the SCHANNEL settings to OS defaults at first startup

Change log

2011

- Fixed Protocol initialization on Vista/Seven/2008/2008R2 (Reported by Adrian F. Dimcev)
- Fixed TLS 1.1 displayed on Vista/2008 (Reported by Adrian F. Dimcev)

2013

- Added Windows 8 support
- Added Windows Server 2012 support
- Resolved an issue around P521 additions

Download

Harden SSL/TLS can be found under

http://www.g-sec.lu/products.html
http://blog.zoller.lu

Limitation of Liability

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts), shall Thierry Zoller or G-SEC .ltd be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses),even if such Contributor has been advised of the possibility of such damages.