SSL Web Server and Client Configuration

Matthew J. Fanto
matthew.fanto@nist.gov
Computer Security Division
National Institute of Standards and Technology
Introduction

- SSL/TLS provide a method of entity authentication as well as encrypted communications
- Client proposes, server disposes
- Client should protect itself and not allow connection unless a FIPS approved algorithm is being used.
The issue

- FIPS Approved Algorithms
  - Triple DES or AES Encryption
  - SHA-1 hashes or HMAC
- Can common servers & clients be set to use only FIPS approved algorithms?
  - What do you have to do?
  - What are the limitations and side effects?
Disclaimer

- NIST does not endorse or recommend any of the software or products mentioned in this talk.
- We did not consider whether the products used validated crypto modules or not.
- We tested the interoperability of clients (browsers) and servers when configured to use cipher suites with FIPS approved algorithms, but did not test the correctness of TLS implementations.
Server Statistics

- Servers were picked based on usage.
- Statistics available at [http://www.netcraft.com](http://www.netcraft.com)

<table>
<thead>
<tr>
<th>Product</th>
<th>Usage</th>
<th>Percent</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apache</td>
<td>21,120,388</td>
<td>56.21%</td>
</tr>
<tr>
<td>Microsoft IIS</td>
<td>11,902,821</td>
<td>31.68%</td>
</tr>
<tr>
<td>Zeus</td>
<td>849,089</td>
<td>2.26%</td>
</tr>
<tr>
<td>iPlanet</td>
<td>824,245</td>
<td>2.19%</td>
</tr>
</tbody>
</table>
Apache 2.0.35

• FIPS compliance
  • EDH-RSA-DES-CBC3-SHA
  • EDH-DSS-DES-CBC3-SHA
  • DES-CBC3-SHA
  • ADH-DES-CBC3-SHA

• Configuration
  • conf/ssl.conf
  • SSLCipherSuite ‘3DES:!MD5’
Microsoft IIS 4.0

- FIPS Compliance
  - DES-CBC3-SHA
  - Special patch needed for Diffie-Hellman
  - Prefers RC4 algorithm – will select if the client offers it

- Configuration
  - Must edit the registry to disable ciphers
    - NIST developing utility
  - Affects all applications that use crypto service provider
Zeus Web Server 4.0

- FIPS Compliance
  - Does not support any FIPS based cipher suites
- Configuration
  - No configuration options
iPlanet 6.0

- FIPS Compliance
  - DES-CBC3-SHA
  - FIPS-140 DES-CBC3-SHA
    - Netscape specific cipher suite
- Configuration
  - Easy to use interface. Enable ciphers with mouse.
Internet Explorer 6.0

- FIPS Compliance
- Supports DES-CBC3-SHA but prefers RC4
- Configuration
  - Must edit the registry to disable ciphers
  - NIST developing utility
  - Affects all applications that use crypto service provider
Netscape Navigator 6.2

- FIPS Compliance
- DES-CBC3-SHA
- FIPS-140 DES-CBC3-SHA
- Netscape specific cipher suite
- Configuration
- Easy to use interface. Enable ciphers with mouse.
Mozilla 1.1a

- FIPS Compliance
- DES-CBC3-SHA
- FIPS-140 DES-CBC3-SHA
- Netscape specific cipher suite
- Configuration
- Easy to use interface. Enable ciphers with mouse.
Opera 6.03

- FIPS Compliance
  - DES-CBC3-SHA
- Configuration
  - Highlight allowed ciphers
Conclusion

- Can configure most products to do only 3-DES
- Apache supports most number of FIPS compliant cipher suites
- Apache allows changing cipher suite preference (if client cannot do 3DES, fall back to RC4)
- No tested client contains preference list
- The only way to ensure that FIPS compliant ciphers are being used in a SSL/TLS connection is to force either the client or the server to allow only 3DES and SHA-1.
Questions and Answers