

# Re: SSL Scanner

---

*Source:* <http://www.derkeiler.com/Newsgroups/alt.computer.security/2007-10/msg00093.html>

---

- *From:* royend <royend@xxxxxxxx>
  - *Date:* Sun, 28 Oct 2007 03:50:21 -0700
- 

On 28 Okt, 04:49, Solbu <so...@xxxxxxxxxxxxxxxx> wrote:

-----BEGIN PGP SIGNED MESSAGE-----  
Hash: SHA1

royend sent the following transmission through subspace:

the project focuses on the vulnerability of  
the web, and I am hoping to shove that even though SSL is implemented  
the packages might be vulnerable to a Man-In-The-Middle-Attack (please  
correct me if I am wrong), as the packages might be intercepted by an  
attacker.

If someone intercepts the packages using a man-in-the-middle-attack,  
the encryption will break, thus alerting the user.

You cannot intercept encrypted packages  
without alerting the user that someone IS intercepting them.  
Because the certificate will be wrong.

---  
Solbu -<http://www.solbu.net>  
Remove 'ugyldig.' for email  
PGP key ID: 0xFA687324  
-----BEGIN PGP SIGNATURE-----  
Version: GnuPG v1.2.2 (GNU/Linux)

iD8DBQFHJAbBT1rWTfpocyQRAqGlAKCxpRbRHcfiYKUr10lkzQ9BBC1siwCg9/fW  
ZpxgxPOj+WIKQd7tmRv8fSo=  
=wwIT  
-----END PGP SIGNATURE-----

On 28 Okt, 11:29, Jim Watt <jimw...@xxxxxxxx> wrote:

On Sat, 27 Oct 2007 08:22:11 -0700, royend <roy...@xxxxxxxx> wrote:

Re: SSL Scanner

Is there any programs you would recommend which will handle SSL/TLS?  
Would for instance a program like Ethereal be able to read packages  
using SSL protocols?

Explanation why it can't be done...

--

Jim Watt <http://www.gibnet.com>

That is what I thought (and hoped for...)  
Can the packages be saved when intercepted and without changing the  
package be used in a replay attack?

royend.

.