APACHE SECURED BY SSL
Apache-SSL

Team A.L. Digital & Apache-SSL February 5, 2000

조대현, cool@hansaram.sarang.net

v0.3 2000년 2월 20일

이 문서는 https://www.apache-ssl.org/ 의 내용을 번역(?) 한 것입니다.

목 록

1 Main Features

- 상업 비상업적 이용 가능
- 세계 어디서나 128비트 인크립션이 가능
- 클라이언트 증명
- 전체 소스 코드
- 확장가능한 모듈형식의 API

2 Apache-SSL이란?

Apache-SSL은 `Apache`와 `SSLeay/OpenSSL`을 기반으로 하는 보안 웹서버이다. 이것은 BSD 형식의 `license`에 기반한다. 간단히 copyright notices만 유지한다면 상업적이든 비 상업적이든 공짜로 쓸수 있단 말이다(단지 서버를 돌리기 전에 `SSLeayIsthislegal?FAQ`는 읽어 보길 권한다). This is the same license as used by Apache from version 0.8.15

3 다운로드

현재 릴리즈: `Apache_1.3.11+ssl_1.38` 릴리즈 날짜: `2000년 1월 25일`

당신은 또한 `openssl-0.9.4`가 필요하고 서 구할 수 있다.

Apache-SSL 소스 패치는 다음 UK 마스터 배포 사이트에서 구할 수 있다:

- `OxfordUniversity.`
- `UniversityofCambridgeComputerLaboratory`와

다른 FTP 미러 사이트들:

- `ftp.zedz.net` (The Netherlands)
- `ftp.win.ne.jp` (Japan)
- `ftp.sage-au.org.au` (Australia)
- `ftp.vwv.com` (South Africa)

- mirror.aarnet.edu.au (Australia)
- ftp.it.net.au (Australia)
- ftp.infoscience.co.jp (Japan)
- ftp.funet.fi (Finland)
- apache-ssl.raver.net (Canada)
- ftp.pca.dfn.de (Germany)
- ftp.sekure.net (Sweden)
- ftp.clinet.fi (Finland)
- opensores.thebunker.net (UK)
- ftp.gin.cz (CZ)

또는 HTTP 미러 사이트들:

- mirror.aarnet.edu.au (Australia)
- ftp.it.net.au (Australia)

O/S specific 버전들:

- RedHat, Caldera 그리고 TurboLinux 소스와 실행가능한 .rpm 들 역시 뒤에 나열된 모든 서버의 contrib/rpms 디렉토리에서 찾을 수 있다.
- 포트 있는 곳: http://www.freebsd.org/ports/www.html.

4 필요한 것은?

필요한 것들은 (1.2.0+ 과 1.3.0+ 버전에서 가능)용 패치와 몇개의 특별한 소스 파일, 아주 조금의 README 와 설정 예제 파일들이다. 패치는 아파치 소스에 적용된 후에 컴파일 되고, SSLeay(0.5.1b+) 또는 OpenSSL과 연결된다. The modified source will still compile a standard Apache as well as Apache-SSL.

5 최신으로 유지하기

업그레이드를 가장 잘 알 수 있는 방법은 가장 최신의 버전을 알려주는 발표(announce) 에 가입하는 것이다.

6 벌레 잡기와 패치

벌레나 개선사항은 ben@algroup.co.uk로 보내라.

버그나 문제점들을 레포팅하는데 부담을 느끼지 마라. 그러나, (당신이 돈을 지불할 의사가 있더라도.. –;) 약속(고친다는?)은 못하겠다.

7 상업적 지원

아파치나 Apache-SSL 둘다 상업적인 지원이 가능하다. 흥미 있거든 ben@algroup.co.uk로 메일을 보내라.

8 전자 증명

다음은 페이지 링크를 요청해온 회사들이다. 나는 아래 단체들을 보증, 추천하지도 않고 나와의 관계 역시 전혀 없다. 요청한 순으로 나열하였다.

Apache-SSL용 전자 증명이 가능한 곳들:

- Thawte Consulting, at http://www.thawte.com/certs/server/request.html
- CertiSign Certificadora Digital Ltda., at http://www.certisign.com.br/
- IKS GmbH, at http://www.iks-jena.de/produkte/ca/
- BelSign NV/SA, at http://www.belsign.be/
- VeriSign, Inc. at http://www.verisign.com/guide/apache/
- TC TrustCenter (Germany) at http://www.trustcenter.de/html/Produkte/TC_Server/855.htm
- NLsign B.V. at http://www.nlsign.nl/
- Deutsches Forschungsnetz at http://www.pca.dfn.de/dfnpca/certify/ssl/
- 128i Ltd. (New Zealand) at http://www.128i.com/
- Entrust.net Ltd. at http://www.entrust.net/products/index.htm
- Equifax Inc. at http://www.equifaxsecure.com/ebusinessid/
- GlovalSign NV/SA at http://www.globalsign.net/
- 물론 당신의 사이트도 넣을 수 있다.

9 PGP 키(key)

나에게 사적인 메일을 보낼려면, 내 PGP키가 있다. 제발 빌요한 데만 써달라; 나는 패스문(passphrase) 타이핑이 정말 싫다.. -+

10 FAQ

10.1 Apache-SSL 은 한동안 업데이트 되지 않았다 - 이건 낡았다(out-of-date)는 말인가?

아니다, 위말은 그것(Apache-SSL)이 사람들이 원하는 만큼 잘 작동한다는 뜻이다. 우리는 고쳐져야 할 버그가 있을때와 새 버전의 Apache(이하 아파치)가 나올때, 또는 누군가가 새로운 기능을 원할때만 업데이트 한다.

10.2 내 브라우저는 왜 Apache-SSL에 접속할 때 멈춰있기만 하나?

`https:` 대신에 `http:`를 사용했기 때문이다. 또, 에러 로그에서 다음 메시지를 본게 된다면 역시 위와같은 이유에서다.

```
SSL_Accept failed error:140760EB:SSL routines:SSL23_GET_CLIENT_HELLO:unknown protocol
```

10.3 패치가 적용이 안되는데, 뭐가 잘못된건가?

다음과 같은 결과를 얻는다면,

```
$patch < SSLpatch
  Looks like a new-style context diff.
  File to patch:
```

아마 옛날 버전의 patch를 가지고 있을 것이다. 2.1 이상의 버전으로 바꾸고 다시 시도하라.

10.4 HTTP가 포트(port) 80을 쓰는건 아는데, HTTPS는?

당신은 HTTPS를 아무 포트에서나 돌릴 수 있지만, 대부분의 브라우저가 기본으로 찾는 표준 포트는 443이다. 너(헉.. 언제부터.. –;)는 다음과 같이 URL에 포트번호를 지정해서 브라우저가 강제로 찾도록 할 수 있다.

```
https://secure.server.hell:666
```

10.5 나는 한 머신에서 보안(secure), 비보안(non-secure) 서버를 같이 돌리고 싶다. 가능한가?

두가지 방법이 있다. 두개의 서버 대몬을 돌리거나, 한 대몬에서 두가지 서비스를 동시에 하거나. 두 대몬를 돌리는 좋은 이유가 있더라도, 보통 가장 간단하게 한 서버를 돌리고 SSL이 필요없는 부분은 가상호스트(virtual host)로 그 기능을 꺼버리면 된다. 만약 두개의 대몬을 돌리고 싶다면 각 서버가 정해진 포트(보통 비보안은 포트 80, 보안은 443) 하고만 연결 되도록 해야 한다. 하나의 서버만 돌리고 싶다면, 어떻게 설정하는지 여기 설정 파일이 있다.

10.6 이제 막 서버를 설치 했다. 테스트 증명서는 어떻게 만드나?

단계 하나 - 키(key)와 요청(request, 청, 청구.. 머야.. –;)를 만들어라.

```
  openssl req -new > new.cert.csr
```

단계 둘 - 키에서 패스문(passphrase)를 지워라(선택사항이다).

```
  openssl rsa -in privkey.pem -out new.cert.key
```

단계 셋 - 요청(request)을 서명된 증명(cert)으로 바꿔라.(바꿔, 바꿔, ^^;)

```
  openssl x509 -in new.cert.csr -out neww.cert.cert -req -signkey new.cert.key -days 365
```

위 결과를 Apache-SSL의 지시자로 다음과 같이 사용한다.

```
  SSLCertificateFile /path/to/certs/new.cert.cert
  SSLCertificateKeyFile /path/to/certs/new.cert.key
```

10.7 클라이언트 증명서는 어떻게 만드나?

단계 하나 - 위 처럼 CA 증명/키 쌍을 만든다.

단계 둘 - CA 키로 고객 요청에 서명한다.

```
openssl x509 -req -in client.cert.csr -out client.cert.cert -signkey my.CA.key -CA my.CA.cert -CAkey my.CA.key -CAcreateserial -days 365
```

단계 셋 - 'client.cert.cert' 파일을 요청하는이에게 넘겨주라.

Apache-SSL은 다음을 추가 함으로써 이 증명서의 확인이 가능하다.

```
SSLCACertificateFile /path/to/certs/my.CA.cert
SSLVerifyClient 2
```

10.8 내 CGI로 어떻게 클라이언트 증명에 접근하는가?

릴리즈 apache_1.3.2+ssl_1.27 이상에서는 다음 지시자를 사용한다.

```
SSLExportClientCertificates
```

이것은 클라이언트 증명의 내용을 포함하는 환경변수를 만들게 된다. 더 자세한 것은, docs 섹션의 SSLExportClientCertificates를 보라. 작동 예제도 있다: https://www.apache-ssl.org/cgi/cert-export

10.9 FontPage98 Extensions with Apache-SSL은 어떻게 설치하나?

Bertrand Renuart가 이에 대한 자세한 내용을 http://www.itma.lu/howto/apache에서 기술하고 있다.

10.10 Verisign cert를 설치할 때, 왜 "getca", "getverisign"을 찾을 수 없는가?

Apache-SSL 명령에서 Verisign은 지원되지 않기 때문이다. 사용하고 싶다면 Stronghold(상용 아파치 기반 SSL 지원 서버)를 사용해라. 당신이 해야 할 일은 단지 증명을 파일에 저장하고 그 이름을 SSLCertificateFile지시자에 넘겨주면 된다. 키파일도 넘겨야 하는걸 기억해라.

10.11 일반적인 컴파일 에러

```
gcc -c  -I../os/unix -I../include -I/usr/local/ssl/include   -funsigned-char -DTARGET=\"httpsd\" -DAPACHE_SSL `../apaci` -DAPACHE_SSL buff.c
buff.c: In function `ap_read':
buff.c:259: structure has no member named `stats'
buff.c:267: structure has no member named `stats'
buff.c:268: structure has no member named `stats'
buff.c:269: structure has no member named `stats'
buff.c:271: structure has no member named `stats'
buff.c: In function `ap_write':
buff.c:346: warning: passing arg 2 of `SSL_write' discards `const' from pointer target type
*** Error code 1
```

OpenSSL을 업그레이드 해야 한다.

10.12 Y2K 문제는?

Apache-SSL 하부의 컴포넌트에는 날짜관련 처리가 없어서 당신 시스템의 전체적인 컴플라이언스(compliance)엔 영향을 받지 않는다. 메인 컴포넌트인 아파치는 Y2K에 대해서 이야기 하고 있다. 또한 당신은 OS, 하드웨어와 다른 모듈을 검사해야 한다.

11 메일링 리스트

두 Apache-SSL 메일링 리스트가 있다. Apache-SSL 커뮤니티(community)로부터 일반적인 도움이나 지원을 원하면, apache-ssl-help@lists.aldigital.co.uk로 빈 메일을 보내라. 이것은 질문에 대한 해답을 얻는 가장 빠른 경로 일 것이다. 그러나, 질문을 포스팅하기전에 archive에 답이 있는지부터 확인해라.

단순히 최신으로 유지하고 새 릴리즈와 중요한 발표를 듣기만을 원한다면, apache-sslannounce-help@lists.aldigital.co.uk가 있다.

12 Apache-SSL은 mod_ssl이 아니다!!

There appears to be some confusion regarding Apache-SSL and mod_ssl. To set the record straight: mod_ssl is not a replacement for Apache-SSL - it is an alternative, in the same way that Apache is an alternative to Netscape/Microsoft servers, or Linux is an alternative to FreeBSD. It is a matter of personal choice as to which you run. mod_ssl is what is known as a 'split' - i.e. it was originally derived from Apache-SSL, but has been extensively redeveloped so the code now bears little relation to the original.

Apache-SSL continues to be developed and maintained, our main focus being on reliability, security and performance, rather than features and bells and whistles. I hope this makes things clear. *(Adam Laurie)*

13 링크들

관련 웹 자원들:

- PeterGutmann'sSecurityandEncryption-relatedResourcesandLinks
- AndrewFord'sApache/Apache-SSLQuickReferenceCard

14 미러 웹사이트

- Infoscience, Japan (Japanese language), at japache.infoscience.co.jp/Apache-SSL/Apache-SSL.html.
- BilkentUniversity, Ankara, Turkey, at http://sunsite.bcc.bilkent.edu.tr/pub/infosystems/apache-ssl/Index.html.
- raver.net, Canada, at http://apache-ssl.raver.net/.
- algroup, USA, at http://lynx.usa.algroup.co.uk/mirrors/www.apache-ssl.org/.
- instinct.org, Czech Republic, at http://www.instinct.org/apache-ssl/
- gin.cz, CZ, at http://apache-ssl.gin.cz/

15 크레디트(^^;)

Apache-SSL was written by BenLaurie, who is also an Apachecoreteammember, and an OpenSSLcoreteammember.

The development of Apache-SSL is sponsored by A.L.DigitalLtd., and this site is hosted by tem.

Info on FTP mirror sites, CAs, Links, etc., should be send to: `TheWebSlaves`.

Apache-SSL graphics courtesy of `JamieHarrison` and `TheWoWFoundation`, based on the original feather by `RandyTerbush`. Feel free to replicate.

16 Team A.L. Digital & Apache SSL

A.L. Digital Ltd. participate in the Distributed Net encryption cracking efforts, as do many of our friends. To see how our team is doing, click the team logo above. To read more about the project, click on the banner above. To join our team, affiliate yourself with team no. 5209. For your personal privacy, the team membership listing is not open to the public, and we promise not to use it ourselves. For anything.