Introduzione ad OpenSSL

Alfredo De Santis

Dipartimento di Informatica
Università di Salerno

ads@unisa.it

Maggio 2020

Outline

- Caratteristiche Generali
- Versioning
- Funzionalità di Help
- Comandi OpenSSL
- Ambiente di Lavoro

Outline

- **Caratteristiche Generali**
- Versioning
- Funzionalità di Help
- Comandi OpenSSL
- Ambiente di Lavoro

OpenSSL
Caratteristiche Generali

- Progetto Open Source nato nel dicembre del 1998
- OpenSSL fornisce implementazioni per
  - Funzioni Crittografiche (o Primitive)
  - Protocolli quali Secure Sockets Layer (SSL) e Transport Layer Security (TLS)

"The Swiss Army knife of cryptography"

OpenSSL
Cryptography and SSL/TLS Toolkit

OpenSSL
Caratteristiche Generali

- OpenSSL comprende
  - Comandi eseguibili per funzioni e protocolli crittografici
  - Libreria contenente API per sviluppare applicazioni crittografiche
- OpenSSL supporta crittografia basata su Curve Ellittiche
  - Elliptic Curve Cryptography (ECC)

"The Swiss Army knife of cryptography"

OpenSSL
Cryptography and SSL/TLS Toolkit

OpenSSL
Caratteristiche Generali

- OpenSSL si occupa di
  - Creazione e gestione di chiavi private, chiavi pubbliche e parametri
  - Operazioni crittografiche a chiave pubblica
  - Creazione di certificati X.509, Certificate Signing Request (CSR) e Certificate Revocation List (CRL)
  - Calcolo di Message Digest
  - Cifratura e decifratura mediante cifrari
  - Testing di client e server SSL/TLS
  - Gestione di e-mail firmate o cifrate
  - Richieste di Time Stamp, generazione e verifica

"The Swiss Army knife of cryptography"

OpenSSL
Cryptography and SSL/TLS Toolkit

Outline

- Caratteristiche Generali
- **Versioning**
- Funzionalità di Help
- Comandi OpenSSL
- Ambiente di Lavoro

OpenSSL
Versioning

- OpenSSL utilizza il seguente formato per distinguere le sue versioni: $n_1.n_2.n_3c$, dove
  - $n_1.n_2.n_3$ sono numeri
  - c, se presente, è costituita da una o più lettere
  - **Esempio:** 10.0.2g

- Tale formato si basa su uno specifico schema di versioning definito da OpenSSL

OpenSSL
Cryptography and SSL/TLS Toolkit

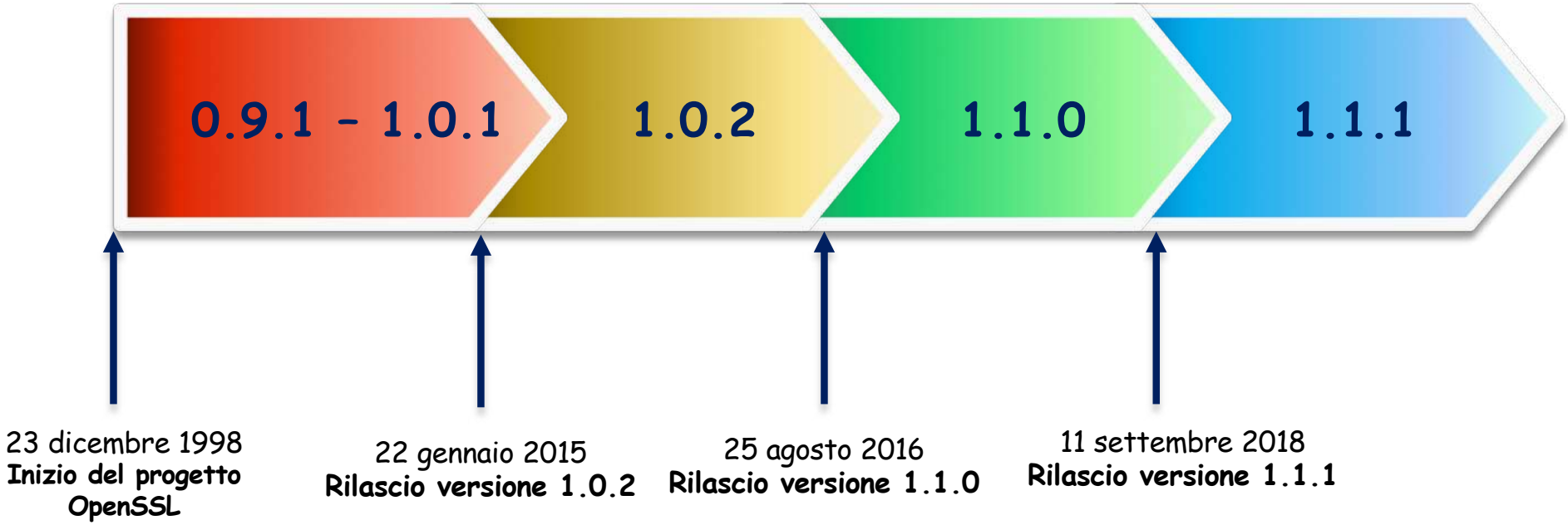
OpenSSL
Versioning

$n_1.n_2.n_3c$

- OpenSSL adotta il seguente schema di versioning
  - **Major releases** cambiano una o entrambe le prime due cifre
    - Possono rompere la compatibilità con le versioni precedenti
  - **Minor releases** cambiano l'ultima cifra, ad es. 1.1.0 e 1.1.1
    - Possono contenere nuove funzionalità
    - Di solito sono retro-compatibili con le versioni precedenti
  - **Letter releases** contengono esclusivamente correzioni di bug e/o di sicurezza
    - Non contengono nuove funzionalità

OpenSSL
Cryptography and SSL/TLS Toolkit

OpenSSL
Versioning



Supporto

- Non più supportate
- Supporto fino al 31 dicembre 2019 (*Long Term Support*)
- Supporto fino al 11 settembre 2019
- Supporto fino al 11 settembre 2023 (*Long Term Support*)

Outline

- Caratteristiche Generali
- Versioning
- **Funzionalità di Help**
- Comandi OpenSSL
- Ambiente di Lavoro

OpenSSL
Help

- Documentazione
  https://www.openssl.org/docs/

- Manpage
  https://www.openssl.org/docs/manmaster/man1/openssl.html

- Cookbook (free download)
  https://www.feistyduck.com/books/openssl-cookbook/

- Mailing list
  https://www.openssl.org/community/mailinglists.html

OpenSSL Wiki

https://wiki.openssl.org/index.php/Main_Page

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview	Compilation and Installation	Internals	Mailing Lists
libcrypto API	libssl API	Examples	Index of all API functions
License	Command Line Utilities	Related Links	Binaries
SSL and TLS Protocols	1.1 API Changes	FIPS modules	

OpenSSL Wiki

https://wiki.openssl.org/index.php/Main_Page

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [ed

Panoramica generale su OpenSSL

OpenSSL Overview
libcrypto API
License
SSL and TLS Protocols

Mailing Lists
Index of all API functions

OpenSSL Overview

OpenSSL is a versatile tool that can be used for many purposes.

OpenSSL provides:

- A command line application to perform a wide variety of cryptography tasks, such as creating and handling certificates and related files. OpenSSL commands
- A comprehensive and extensive cryptographic library libcrypto.
- A library for enabling SSL/TLS communications libssl to provide SSL and TLS Protocols support within clients or servers applications.

Command Line [edit]

Example uses of the OpenSSL command line tool include:

- Creating and handling certificates and related files. openssl commands. A beginners introduction to certificates is on the Certificate Lifecycle page.
- Testing of SSL/TLS protocols (openssl s_server, openssl s_client).

History [edit]

History And People

OpenSSL Wiki

https://wiki.openssl.org/index.php/Main_Page

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn among multiple locations and formats.

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview
libcrypto API
License
SSL and TLS Protocols

Informazioni sul protocollo SSL/TLS implementato da OpenSSL

SSL and TLS Protocols

SSL stands for Secure Sockets Layer and was originally created by Netscape. SSLv2 and SSLv3 are the 2 versions of this protocol (SSLv1 was never publicly release). After SSLv3, SSL was renamed to TLS.

TLS stands for Transport Layer Security and started with TLSv1.0 which is an upgraded version of SSLv3.

Those protocols are standardized and described by RFCs.

OpenSSL provides an implementation for those protocols and is often used as the reference implementation for any new feature.

The goal of SSL was to provide secure communication using classical TCP sockets with very few changes in API usage of sockets to be able to leverage security on existing TCP socket code.

SSL/TLS is used in every browser worldwide to provide https (http secure) functionality.

The latest standard version is TLSv1.2 http://tools.ietf.org/html/rfc5246, while the upcoming TLS v1.3 is still draft.

Connectionless support is provided via DTLS.

Those protocols are configurable and can use various ciphers depending on their version.

Contents [hide]

OpenSSL Wiki

https://wiki.openssl.org/index.php/M

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Wel valued.

This wiki is intended as a place for collecting, organizing, and refining useful information about OpenSSL that is currently strewn amo

Contents [hide]

OpenSSL Quick Links [edit]

OpenSSL Overview	Compilation and Installation	
libcrypto API	libssl API	
License	Command Line Utilities	
SSL and TLS Protocols	1.1 API Changes	FIPS modules

Funzionalità offerte da OpenSSL mediante linea di comando

Command Line Utilities

OpenSSL site command line tools

Contents [hide]

Getting started with your openssl toolkit [edit]

OpenSSL Wiki

https://wiki.openssl.org/index.php/Main_Page

Main Page

This is the OpenSSL wiki. The main site is https://www.openssl.org . If this is your first visit or to get an account please see the Welcome page. Your participation and Contributions are valued.

This wiki is intended as a place for co

Contents [hide]

OpenSSL Quick Links [e

OpenSSL Overview	Compilation and Installation	Internals	Ma
libcrypto API	libssl API	Examples	In
License	Command Line Utilities	Related Links	Bi
SSL and TLS Protocols	1.1 API Changes	FIPS modules	

FIPS modules

There is currently only one extant FIPS 140-2 validated cryptographic module, the *OpenSSL FIPS Object Module 2.0*. This module is revised periodically with platform portability modifications to support additional platforms (general improvements and bugfixes, even security vulnerability mitigations, are not permitted[1]). As of September 2016 the latest module revision is 2.0.13.

The 2.0 module is rather confusingly covered by three very similar validations, the original #1747[2] and the "Alternative Scenario 1A" clone validations #2398 [3] and #2473 [4]. For perverse and inscrutable bureaucratic reasons the #1747 validation cannot be updated and it and #2473 will forever remain at revision 2.0.10. New platforms can be added to #2398 for revision 2.0.10, and new platforms and new revisions can currently be added to the #2398 validation. The choice of validation is a paperwork consideration as all three validations reference the same cryptographic module. Note there are also a number of third party clone validations that also reference exactly the same cryptographic module. Since that module is available under the OpenSSL open source license, any such validation can be cited for satisfying FIPS 140-2 validation requirements. Collectively across all such validations the 2.0 FIPS module has more than two hundred formally tested platforms (known as "Operational Environments" in FIPS-speak). More information about the 2.0 FIPS module can be founf starting at FIPS_module_2.0.

The 2.0 FIPS module is compatible with OpenSSL releases 1.0.1 and 1.0.2, and no others. The extensive internal structural changes for OpenSSL 1.1 preclude the use of the 2.0 FIPS module with that release.

A new validation effort is to develop and validate a new open source based cryptographic module was announced in July 2016[5]. This new module will be usable with OpenSSL release 1.1. It will provisionally be called *OpenSSL FIPS Object Module 3.0*. Notes and commentary can be found starting at FIPS_module_3.0.

Compatibilità di OpenSSL con lo standard **Federal Information Processing Standard (FIPS) 140-2** pubblicato dal NIST

http://csrc.nist.gov/groups/STM/cmvp/standards.html

Outline

- Caratteristiche Generali
- Versioning
- Funzionalità di Help
- **Comandi OpenSSL**
- Ambiente di Lavoro

OpenSSL
Comandi

- OpenSSL fornisce
  - Un ampio insieme di comandi
  - Un ancora più ampio insieme di opzioni (parametri)
    - Usate per raffinare e controllare ulteriormente i comandi

OpenSSL™
Cryptography and SSL/TLS Toolkit

Comandi OpenSSL
Modalità Operative

- Mediante il comando **`openssl`** possono essere accedute da command-line tutte le funzionalità offerte da OpenSSL

- Il comando **`openssl`** può essere usato in due *modalità operative*

1. **Interattiva:** Il comando **`openssl`** è invocato senza alcun parametro
   - Viene mostrato un prompt (>) dove digitare i comandi
   - Quando termina l'esecuzione di un comando, il prompt è mostrato di nuovo ed è pronto a processare un nuovo comando
   - Si può uscire da OpenSSL mediante il comando **`quit`**

```
$ openssl
OpenSSL>
```

Comandi OpenSSL
Modalità Operative

- Mediante il comando **`openssl`** possono essere accedute da command-line tutte le funzionalità offerte da OpenSSL

- Il comando **`openssl`** può essere usato in due *modalità operative*

  2. **Batch:** Ciascun comando deve essere preceduto da "**`openssl`**"

```
$ openssl version
OpenSSL 1.1.1  11 Sep 2018
```

Comandi OpenSSL
Sintassi

- La prima parte di un comando OpenSSL è data dal nome del comando stesso, seguito da eventuali opzioni, ciascuna separata da uno spazio
  - Le opzioni di solito iniziano con un trattino e spesso richiedono uno specifico parametro posto dopo uno spazio

- In generale, l'ordine in cui si specificano le opzioni non è significativo
  - Pochi casi in cui l'ordine è significativo
    - Di solito perché una specifica opzione deve apparire sulla command-line come l'ultima opzione specificata

Comandi OpenSSL
Sintassi

- La prima parte di un comando OpenSSL è data dal nome del comando stesso, seguito da eventuali opzioni, ciascuna separata da uno spazio
  - Le opzioni di solito iniziano con un trattino e spesso richiedono uno specifico parametro posto dopo uno spazio

- In generale, l'ordine in cui si specificano le opzioni non è significativo
  - Pochi casi in cui l'ordine è significativo
    - Di solito perché una specifica opzione deve apparire sulla command-line come l'ultima opzione specificata

N.B. Prima di eseguire un determinato **comando**, accertarsi della relativa sintassi, digitando **man comando**

Outline

- Caratteristiche Generali
- Versioning
- Funzionalità di Help
- Comandi OpenSSL
- **Ambiente di Lavoro**

Ambiente di Lavoro per gli Esempi

- Gli esempi mostrati in classe sono stati sviluppati utilizzando il seguente ambiente software
  - Linux Ubuntu 18.04.4 LTS (Long-Term Support)
    - OpenSSL Versione 1.1.1
- È possibile installare Linux Ubuntu
  - Nativamente su una macchina
  - In macchina virtuale (ad es., usando VirtualBox)

Ambiente di Lavoro per gli Esempi

- Gli esempi mostrati in classe sono stati sviluppati utilizzando il seguente ambiente software
  - Linux Ubuntu 18.04.4 LTS (Long-Term Support)
    - OpenSSL Versione 1.1.1

- È possibile installare Linux Ubuntu
  - Nativamente su una macchina
  - In macchina virtuale (ad es., usando VirtualBox)

N.B. L'utilizzo di OpenSSL in un ambiente di lavoro diverso da quello consigliato, potrebbe produrre risultati diversi da quelli mostrati negli esempi

Bibliografia

- OpenSSL Release Strategy
  - https://www.openssl.org/policies/releasestrat.html
- OpenSSL Changelog
  - https://www.openssl.org/news/changelog.html
- OpenSSL Versioning
  - https://wiki.openssl.org/index.php/Versioning

OpenSSL
Cryptography and SSL/TLS Toolkit