Seguridad y Protección de Sistemas Informáticos

Materia: Prácticas
Módulo: Tecnología de la Información

Grado en Ingeniería Informática

UGR 2019/2020

ugr Universidad de Granada

ETSIIT

13 de octubre de 2019

1. OpenSSL
   - Naturaleza
   - Historia

Tabla de Contenidos

1. OpenSSL
   - Naturaleza
   - Historia

Naturaleza

Clave: `OpenSSL` es un proyecto de software libre

`OpenSSL` es una biblioteca de software para aplicar en la comunicación en redes cuando se necesita determinar la identidad de la otra parte o la protección contra el espionaje.

- Es de código abierto y su núcleo está escrito en C.
- Fácil de usar desde un gran número de lenguajes.
- Suministra funciones criptográficas a otros paquetes como `OpenSSH` y navegadores web (para acceso seguro a sitios `HTTPS`)

Naturaleza

Clave: OpenSSL es un proyecto de software libre

OpenSSL es una biblioteca de software para aplicar en la comunicación en redes cuando se necesita determinar la identidad de la otra parte o la protección contra el espionaje.

- Es de código abierto y su núcleo está escrito en C.
- Fácil de usar desde un gran número de lenguajes.
- Suministra funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS)

Naturaleza

Clave: OpenSSL es un proyecto de software libre

OpenSSL es una biblioteca de software para aplicar en la comunicación en redes cuando se necesita determinar la identidad de la otra parte o la protección contra el espionaje.

- Es de código abierto y su núcleo está escrito en C.
- Fácil de usar desde un gran número de lenguajes.
- Suministra funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS)

Naturaleza

Clave: OpenSSL es un proyecto de software libre

OpenSSL es una biblioteca de software para aplicar en la comunicación en redes cuando se necesita determinar la identidad de la otra parte o la protección contra el espionaje.

- Es de código abierto y su núcleo está escrito en C.
- Fácil de usar desde un gran número de lenguajes.
- Suministra funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS)

Naturaleza

- Ayuda al sistema a implementar el *Secure Sockets Layer* (SSL) y otros protocolos de seguridad como el *Transport Layer Security* (TLS).
- OpenSSL también permite crear certificados digitales que pueden ser aplicados en un servidor, por ejemplo Apache.
- Existen versiones disponibles para todos los sistemas basados en Unix (Linux, Solaris, Mac OS X, macOS y los BDS), OpenVMS y Microsoft Windows.
- IBM proporciona un puerto para el System i (OS/400).

Naturaleza

- Ayuda al sistema a implementar el *Secure Sockets Layer* (SSL) y otros protocolos de seguridad como el *Transport Layer Security* (TLS).
- OpenSSL también permite crear certificados digitales que pueden ser aplicados en un servidor, por ejemplo Apache.
- Existen versiones disponibles para todos los sistemas basados en Unix (Linux, Solaris, Mac OS X, macOS y los BDS), OpenVMS y Microsoft Windows.
- IBM proporciona un puerto para el System i (OS/400).

Naturaleza

- Ayuda al sistema a implementar el *Secure Sockets Layer* (SSL) y otros protocolos de seguridad como el *Transport Layer Security* (TLS).
- OpenSSL también permite crear certificados digitales que pueden ser aplicados en un servidor, por ejemplo Apache.
- Existen versiones disponibles para todos los sistemas basados en Unix (Linux, Solaris, Mac OS X, macOS y los BDS), OpenVMS y Microsoft Windows.
- IBM proporciona un puerto para el System i (OS/400).

Naturaleza

- Ayuda al sistema a implementar el *Secure Sockets Layer* (SSL) y otros protocolos de seguridad como el *Transport Layer Security* (TLS).
- OpenSSL también permite crear certificados digitales que pueden ser aplicados en un servidor, por ejemplo Apache.
- Existen versiones disponibles para todos los sistemas basados en Unix (Linux, Solaris, Mac OS X, macOS y los BDS), OpenVMS y Microsoft Windows.
- IBM proporciona un puerto para el System i (OS/400).

Historia

Clave: Fundado en 1998, `OpenSSL` está basado en una distribución de `SSLeay`

que implementan *Eric Andrew Young* y *Tim Hudson*.

- La implementación termina el 17/12/1998, cuando Young y Hudson comienzan a trabajar para *RSA security*.
- El grupo de desarrollo completo consta de 11 miembros, de los cuales 10 son voluntarios; sólo hay un empleado de tiempo completo, Stephen Henson, el desarrollador principal.

Historia

Clave: Fundado en 1998, `OpenSSL` está basado en una distribución de `SSLeay`

que implementan *Eric Andrew Young* y *Tim Hudson*.

- La implementación termina el 17/12/1998, cuando Young y Hudson comienzan a trabajar para *RSA security*.
- El grupo de desarrollo completo consta de 11 miembros, de los cuales 10 son voluntarios; sólo hay un empleado de tiempo completo, Stephen Henson, el desarrollador principal.

Historia

Clave: Fundado en 1998, `OpenSSL` está basado en una distribución de `SSLeay`

que implementan *Eric Andrew Young* y *Tim Hudson*.

- La implementación termina el 17/12/1998, cuando Young y Hudson comienzan a trabajar para *RSA security*.
- El grupo de desarrollo completo consta de 11 miembros, de los cuales 10 son voluntarios; sólo hay un empleado de tiempo completo, Stephen Henson, el desarrollador principal.

Historia

- El proyecto cuenta con un presupuesto de menos de 1 millón de dólores al año y se basa en parte en donaciones.
- Steve Marqués, exconsultor de la CIA en Maryland, comenzó la fundación para gestión de donaciones y contratos de consultoría
- Se obtuvo el patrocinio del Departamento de Seguridad Nacional de Estados Unidos y el Departamento de Defensa de los Estados Unidos.
- En 2013, WikiLeaks publicó documentos obtenidos por Edward Snowden revelando que desde 2010 la NSA había roto con eficacia o puenteado SSL/TLS quizás explotando vulnerabilidades tales como HeartBleed.

Historia

- El proyecto cuenta con un presupuesto de menos de 1 millón de dólores al año y se basa en parte en donaciones.
- Steve Marqués, exconsultor de la CIA en Maryland, comenzó la fundación para gestión de donaciones y contratos de consultoría
- Se obtuvo el patrocinio del Departamento de Seguridad Nacional de Estados Unidos y el Departamento de Defensa de los Estados Unidos.
- En 2013, WikiLeaks publicó documentos obtenidos por Edward Snowden revelando que desde 2010 la NSA había roto con eficacia o puenteado SSL/TLS quizás explotando vulnerabilidades tales como HeartBleed.

Historia

- El proyecto cuenta con un presupuesto de menos de 1 millón de dólores al año y se basa en parte en donaciones.
- Steve Marqués, exconsultor de la CIA en Maryland, comenzó la fundación para gestión de donaciones y contratos de consultoría
- Se obtuvo el patrocinio del Departamento de Seguridad Nacional de Estados Unidos y el Departamento de Defensa de los Estados Unidos.
- En 2013, WikiLeaks publicó documentos obtenidos por Edward Snowden revelando que desde 2010 la NSA había roto con eficacia o puenteado SSL/TLS quizás explotando vulnerabilidades tales como HeartBleed.

Historia

- El proyecto cuenta con un presupuesto de menos de 1 millón de dólores al año y se basa en parte en donaciones.
- Steve Marqués, exconsultor de la CIA en Maryland, comenzó la fundación para gestión de donaciones y contratos de consultoría
- Se obtuvo el patrocinio del Departamento de Seguridad Nacional de Estados Unidos y el Departamento de Defensa de los Estados Unidos.
- En 2013, WikiLeaks publicó documentos obtenidos por Edward Snowden revelando que desde 2010 la NSA había roto con eficacia o puenteado SSL/TLS quizás explotando vulnerabilidades tales como HeartBleed.