Edinburgh College

H16S35 - Managing a Web Server

5
- SSL/TLS
- OpenSSL
- CMS
- WordPress

michael.ferrie@edinburghcollege.ac.uk

CONTENTS

Edinburgh College

SSL - secure sockets layer
TLS - transport layer security

michael.ferrie@edinburghcollege.ac.uk

SSL Security

- SSL provides end-to-end security even if the network is insecure
- Authentication is provided by key pairs
- **Confidentiality** is provided through encryption
- **Integrity** is provided by certificate validation
- **Availability** is provided by the certificate being downloadable from the web server

- ***However***... SSL is no longer in use, as of 2015?

A Brief History of SSL and TLS

- Both are cryptographic protocols that provide authentication encryption between machines over a network
- SSL is the predecessor to TLS - SSL was originally developed by Netscape in 1995 with SSLv2.0 which was quickly replaced by SSLv3.0 in 1996 after several vulnerabilities were found
- TLS is currently at v. 1.3 and was introduced in 1999 as a new version of SSL, based on SSL 3.0
- The differences between TLS and SSL 3.0 are not dramatic

TLS Design

The TLS protocol specification defines two layers:

1) **TLS record** protocol provides connection security

2) **TLS handshake** protocol enables the client and server to authenticate each other and to negotiate security keys before any data is transmitted

- The TLS handshake is a multi-step process, a basic TLS handshake involves the client and server sending “hello” messages, and the exchange of keys, cipher message and a finish message
- TLS is more efficient and secure than SSL as it has stronger message authentication, key-material generation and encryption

SSL or TLS

- SSL 2.0 and 3.0 have been deprecated by the IETF (in 2011 and 2015, respectively)
- Vulnerabilities continue to be discovered in the old SSL protocols (e.g. POODLE, DROWN)
- Modern browsers show a degraded user experience (e.g. line through the padlock or https in the URL bar, security warnings) when they encounter a web server using the old protocols
- You should disable SSL 2.0 and 3.0 in your server configuration, leaving only TLS protocols enabled
- TLS supports pre-shared keys, secure remote passwords, elliptical-curve keys and Kerberos - SSL does not
- TLS and SSL are not interoperable, but TLS does offer backward compatibility for older devices still using SSL

What about SSL certificates?

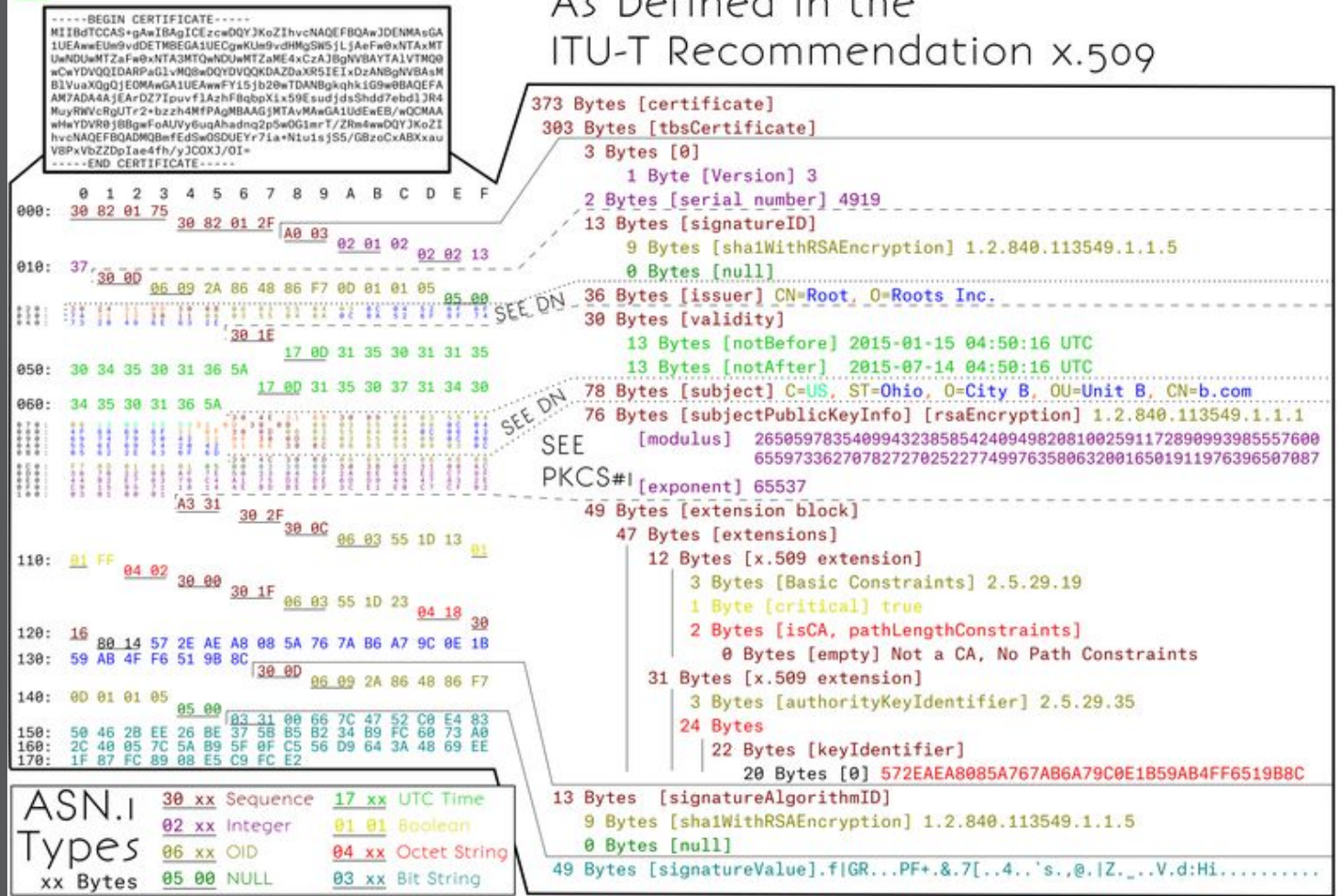
- Certificates ***are not*** the same as protocols, before anyone starts worrying that they need to replace their existing SSL Certificates with TLS Certificates, it's important to note that certificates are not dependent on protocols
- You don't need to use a TLS Certificate vs. an SSL Certificate
- Many vendors use the phrase "SSL/TLS Certificate", it may be more accurate to call them "Certificates for use with SSL and TLS", since the protocols are determined by your server configuration, not the certificates themselves
- You will continue to see certificates referred to as SSL Certificates as that's the term people are familiar with, we are beginning to see increased usage of 'TLS'
- SSL/TLS is a compromise until people become familiar with TLS

X.509 certificate

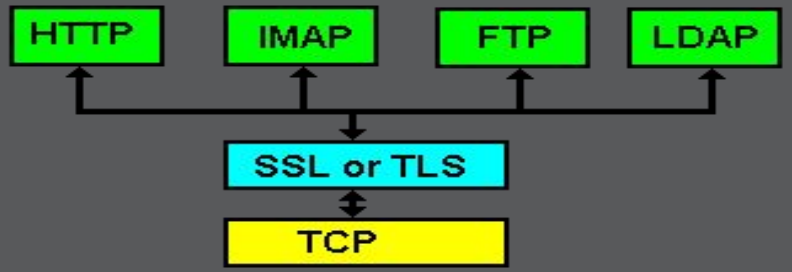
- A standard defining the format of public key certificates, defined by the ITU, based - X.509 certificates are used in many Internet protocols, including TLS/SSL
- X.509 certificates contains a public key and an identity (a hostname, or an individual), and are signed by a certificate authority or self-signed
- When a certificate is signed by a trusted certificate authority, or validated, someone holding that certificate can rely on the public key it contains to establish secure communications with another party, or validate documents digitally signed by the corresponding private key
- X.509 also defines certificate revocation lists, which are a means to distribute information about certificates that have been deemed invalid by a signing authority
- It allows for certificates to be signed by other certificates, eventually reaching a trust anchor

x.509v3 SSL Certificate

As Defined in the ITU-T Recommendation x.509



TLS layer



- Applications that use SSL/TLS really use it as a transport protocol.
- They then use their own data representation and messages and semantics within that "application data"
- Therefore, SSL/TLS cannot be, in the OSI model, beyond layer 4.
- In the OSI model, SSL/TLS must be in layer 6 or 7, and, at the same time, in layer 4 or below.
- The OSI model does not work with SSL/TLS, TLS is not in any layer
- (This does not prevent some people from arbitrarily pushing TLS in a layer. Since it has no practical impact -- this is just a model -- you can conceptually declare that TLS is layer 2, 5, or 17; it won't be proven false.)

OpenSSL

michael.ferrie@edinburghcollege.ac.uk

OpenSSL

- OpenSSL is a software library for applications that secure communications over computer networks against eavesdropping or need to identify the party at the other end
- It is widely used by Internet servers, including most HTTPS websites
- OpenSSL contains an open-source implementation of the SSL and TLS protocols. The core library, written in the C programming language, implements basic cryptographic functions and provides various utility functions
- The OpenSSL Software Foundation (OSF) represents the OpenSSL project in most legal capacities including contributor license agreements, managing donations, and so on.
- OpenSSL is available for most Unix-like operating systems (including Linux, macOS, and BSD) and Microsoft Windows

OpenSSL Commands

- Show version - openssl> `version -a`
- Shows all available commands - openssl> `help`
- All available ciphers - openssl> `ciphers -v`
- List only TLSv1 ciphers - openssl> `ciphers -v -tls1`
- Create a self-signed certificate:

```
openssl req -x509 -newkey rsa:4096 -keyout
keyname.key -out certificatename.crt -days 365
```

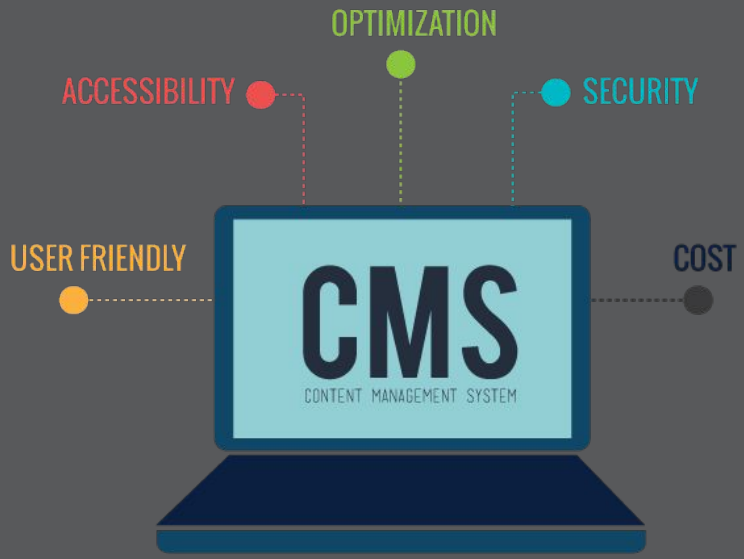
Content management system

michael.ferrie@edinburghcollege.ac.uk

What is a CMS

- A CMS provides website authoring, and administration tools that help users with little knowledge of programming languages create and manage website content
- A WCMS provides the basis for collaboration, giving users the ability to manage documents and output for multiple author editing and participation
- Most systems use a content repository or a database to store page content, metadata
- A presentation layer (template engine) displays the content to website visitors based on a set of templates
- Administration is typically done through browser-based interfaces

Typical CMS features

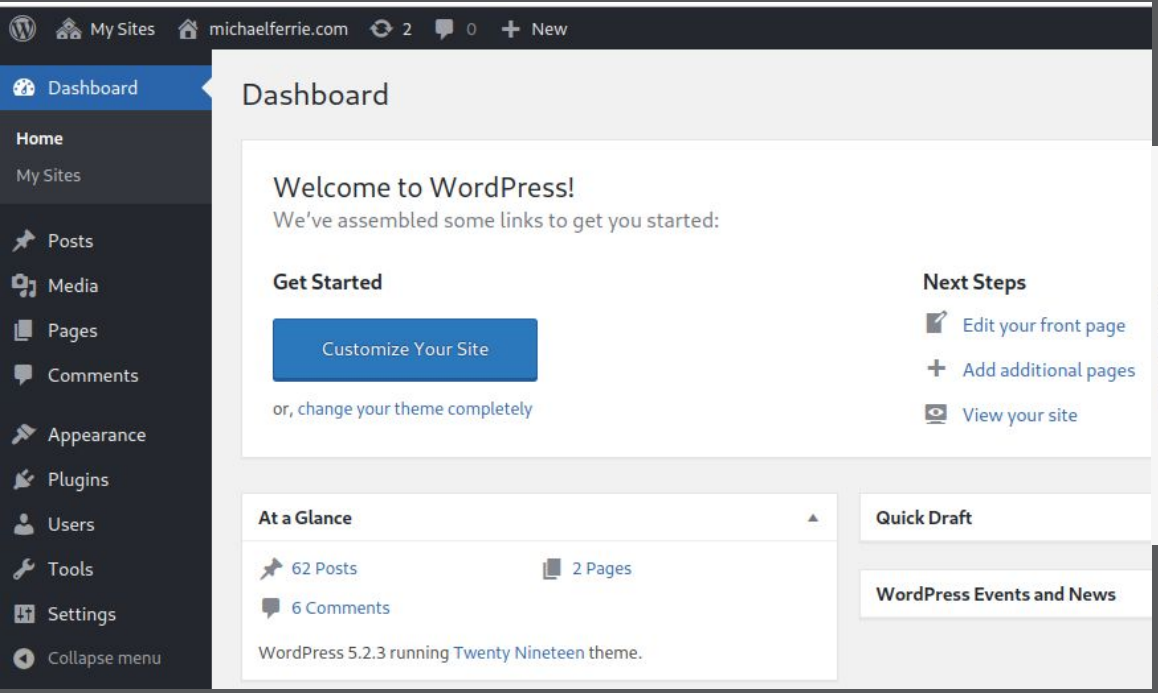


- Search engine optimization (SEO)
- Integrated and online documentation
- Modularity and extensibility
- User and group functionality
- Templating support for changing designs
- Installation and upgrade wizards
- Integrated audit logs
- Compliance with various accessibility frameworks
- Reduced need to code from scratch
- Unified user experience
- Version control
- Edit permission management
- Indexing and search
- Format or style management through themes
- Web-based publishing

Wordpress

- Based on market share statistics, the most popular content management system is WordPress, used by more than 28% of all websites on the Internet, and by 59% of all websites using a known content management system, followed by Joomla and Drupal
- WordPress (WordPress.org) is a (CMS) based on PHP and MySQL that is usually used with the MySQL or MariaDB database servers it includes a plugin architecture and a template system
- It is most associated with blogging but supports other types of web content including more traditional mailing lists and forums, media galleries, and online stores
- Used by more than 60 million websites, including 33.6% of the top 10 million websites as of April 2019, WordPress is the most popular website management system in use

Wordpress dashboard



Edinburgh College

Thanks for listening.
Any questions?

https://www.wpbeginner.com/guides/

michael.ferrie@edinburghcollege.ac.uk