

HTTPS

Secure HTTP

HTTPS

- A combination of HTTP and SSL/TSL.
- Provides
 - authentication of server
 - confidentiality of data
- Often used for secure payment on the Web.
- Default port is 443.

HTTPS

- HTTPS is a URI scheme
 - has identical syntax to the standard HTTP scheme aside from its scheme token.
- HTTPS signals the browser to use an added encryption layer of SSL/TLS to protect the traffic
- Uses Digital Signatures to authenticate servers.

HTTPS – Browser Integration

- Most browsers issue a warning if they receive an incorrect Digital Certificate.
- Also display a warning a site contains a mixture of encrypted and unencrypted content.
- [A certificate can be revoked before it expires if it is compromised.]

HTTPS

- Really HTTP over SSL/TSL.
- Everything in HTTPS requests and responses is encrypted, including headers and body.
- An attacker only can know if there is a connection between the parties.