Web and Mobile Application Security

Chapter 4 — Objectives and Problems of HTTPS

Mr Laïdi FOUGHALI

l.foughali@univ-skikda.dz

(Website ⇒ www.al-moualime.com)

University of Skikda — Computer Science Department

2nd Year Master in Information Security (IS)

Academic Year 2026-2027

Updated on 2026-09-22 at 23:41:19

Outline

Chapter objectives

By the end of this chapter, you will be able to

- Recall how SSL/TLS and the PKI work
- Understand how HTTPS strengthens security
- Identify the limitations and failure modes of HTTPS

4.1 — Recap on the SSL/TLS protocol

HTTPS = HTTP encapsulated in TLS

TLS guarantees three properties:

- **Confidentiality** — encryption of exchanges
- **Integrity** — detection of any tampering
- **Authentication** — of the server (and sometimes the client)

The TLS handshake

Combines **asymmetric** cryptography (authenticate, establish a session key) and **symmetric** cryptography (efficient encryption). Authentication relies on **X.509** certificates issued by CAs within a **PKI**.

4.2 — Strengthening security with HTTPS

Best practices

- **HSTS** (*HTTP Strict Transport Security*) : forces exclusive use of HTTPS
- Systematic HTTP $\rightarrow$ HTTPS redirection
- Recent TLS (1.2/1.3) and *forward secrecy*
- Rigorous certificate management: renewal, revocation, pinning

4.3 — Problems and limitations of HTTPS

Failure modes

- **Forged certificate / compromised CA** : impersonation of a legitimate site
- **MITM and SSL stripping** : downgrade to plain HTTP
- **Mixed content** : HTTP resources on an HTTPS page
- **Validation errors** : self-signed, expired, mismatched certificates
- **Desynchronization with the SOP** : SSL state is not tied to origin (chapter 2)

Key takeaways

The essentials of this chapter

- TLS guarantees confidentiality, integrity, authentication via an asymmetric + symmetric handshake
- Trust relies on X.509 certificates and the PKI
- HTTPS is strengthened by HSTS, recent TLS, and good certificate management
- Weak points: forged certificates, MITM/SSL stripping, mixed content

Questions and exercises

To practice

1. Describe the main steps of a TLS handshake.
2. What is mixed content and why does it weaken an HTTPS page?
3. Explain the role of HSTS against SSL stripping.
4. What checks does the browser perform on a server certificate?