

Confidentiality and Integrity

Threat I: an attacker can eavesdrop messages sent back and forth

Confidentiality: how do exchange information secretly?

Threat 2 : an attacker can tamper messages sent back and forth

Integrity: How do we exchange information reliably?

Confidentiality and Integrity

- Threat I : an attacker can eavesdrop messages sent back and forth
 - Confidentiality: how do exchange information secretly?
- Threat 2: an attacker can tamper messages sent back and forth Integrity: How do we exchange information <u>reliably?</u>

Why and when using HTTPS?

HTTPS = HTTP + TLS

- → TLS provides
 - confidentiality: end-to-end secure channel
 - integrity: authentication handshake
- → HTTPS protects any data send back and forth including:
 - login and password
 - session ID

✓ HTTPS everywhere

HTTPS must be used during the entire session