Confidentiality and Integrity

- Threat 1 : 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 1 : 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?

Generic solution - HTTPS

✓ HTTPS = HTTP + TLS

➡ Transport Layer Security (TLS previously known as SSL) provides

- **confidentiality:** end-to-end secure channel
- **integrity:** authentication handshake