

Confidentiality and Integrity of communications



- ➔ Implement a **virtual trusted channel** over an insecure medium

Storage on an **insecure** medium

➔ Threat 1: **Loss**

An attacker can corrupt or destroy data at rest

➔ Threat 2: **Disclosure**

An attacker can disclose data at rest to other unauthorized parties

➔ Threat 3: **Theft**

An attacker can obtain and store data at an arbitrary location

➔ Threat 4: **Modification**

An attacker can compromise the integrity of data at rest