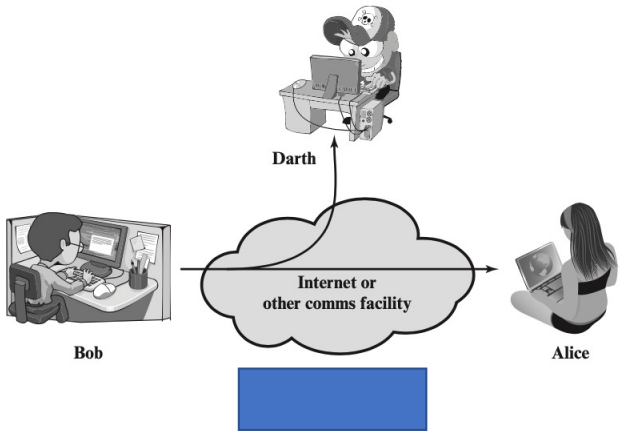
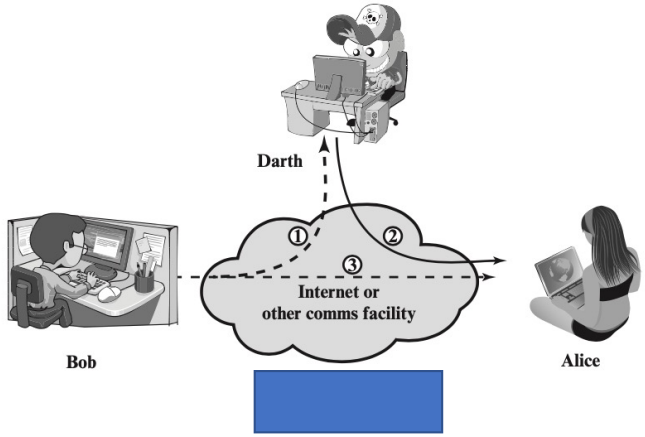
Security attack

- **Definition**: any action that compromises the security of information owned by an organization
- Two types of security attacks
  - Passive attack
  - Active attack





Passive attack

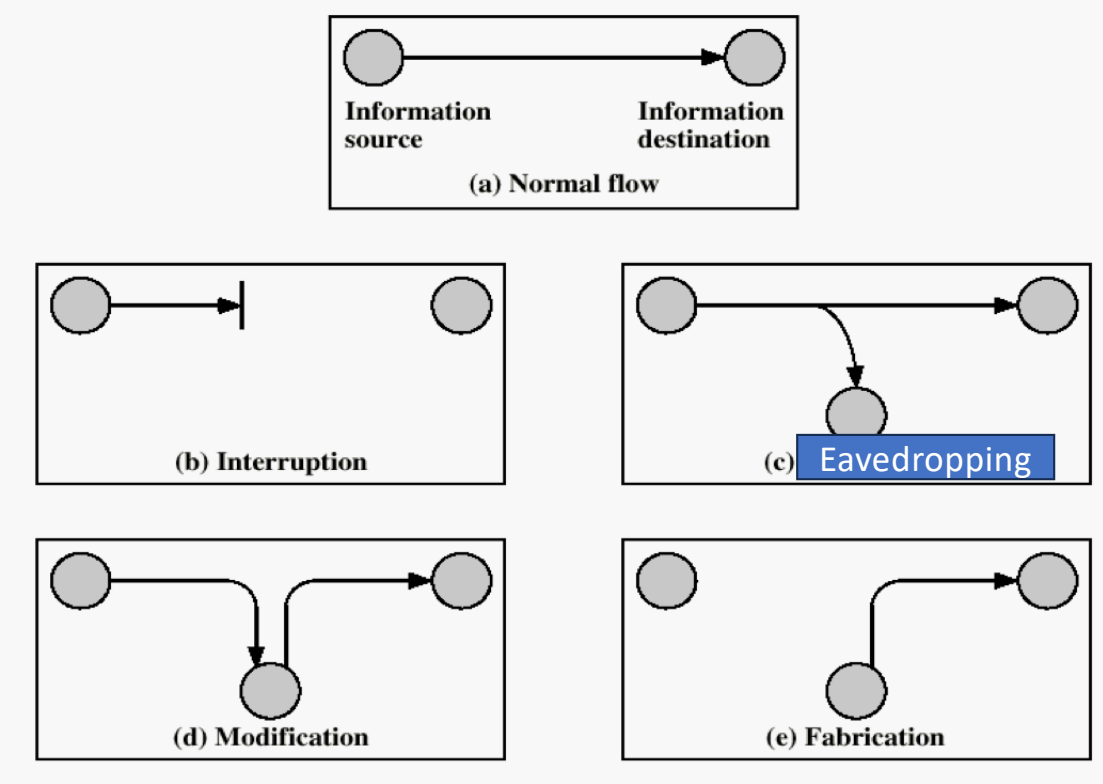
- i.e. eavesdropping on or monitoring of transmissions
- Goal: obtain information being transmitted
  - release of message contents
  - traffic analysis – a promiscuous sniffer
- Very difficult to detect – no alteration of the data
- But easy to prevent, why?

Active attack

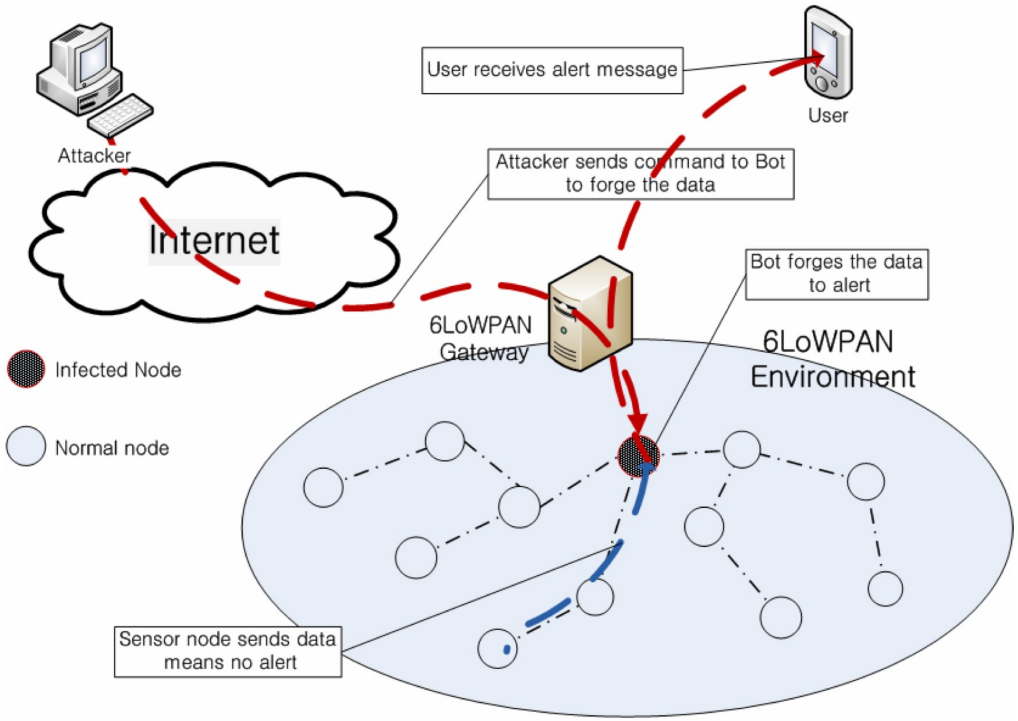
- active attack includes:
  - replay
  - Modification of messages
  - Denial of service
  - Masquerade

Example: two points communication

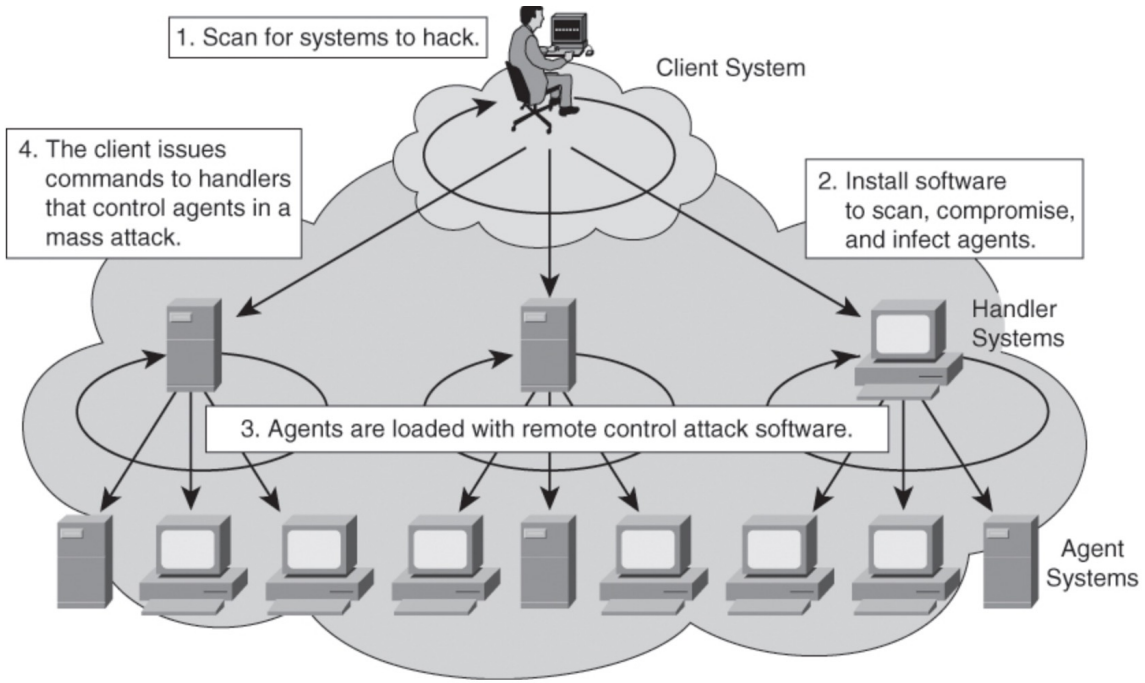
- Generic types of attacks



Example of modification attack in 6LoWPAN



Example: a group of attackers

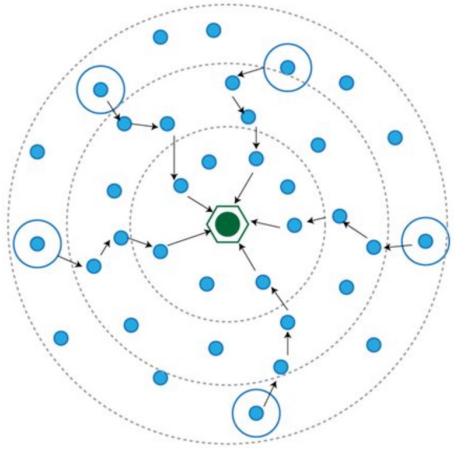


Know Your Threat Model

- **Threat model:** A model of who your attacker is and what resources they have
- One of the best ways to counter an attacker is to attack their reasons

Example: adversary model

- “The adversary is assumed to be intelligent and has limited number of resources. Before capturing the nodes, it exploits the various vulnerabilities of the networks. It knows the topology of the network, routing information. It aims to capture the sink node so as to disrupt the whole traffic. If it is not able to capture the sink node, it will capture the nearby nodes of the sink. It tries to disrupt the whole traffic of the network with minimum number of captured nodes. It is also assumed that the adversary tends to attack more on the nodes closer to the data sink than nodes that are far away”



No class on Wednesday

- No class on Wednesday (Sept 18, 2024) due to the Job fair. Wish you good luck!
- Reminder to form a project group by Sept. 9th, 2024