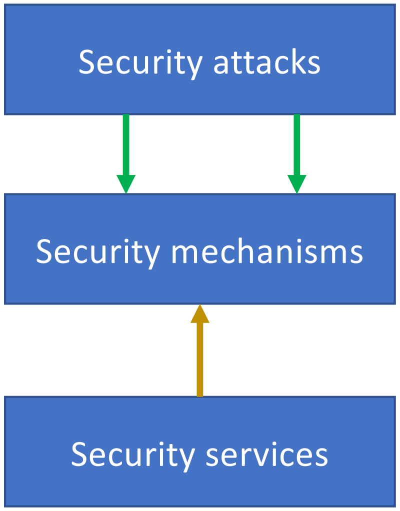
OSI Security Architecture

Attack Model

→ 7 layers

OSI Security Architecture

- International Telecommunication Union – Telecommunication (ITU-T) recommends X.800
- Security Architecture for Open Systems Interconnection (OSI)
  - Defines a systematic way of defining and providing security requirements
  - An international standard



a process (or a device incorporating such a process) to detect, prevent, or recover from an attack

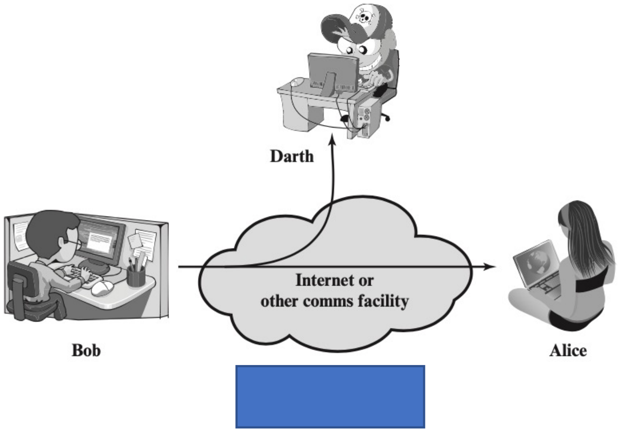
enhances the security of the data processing systems and the information transfers, such as policies

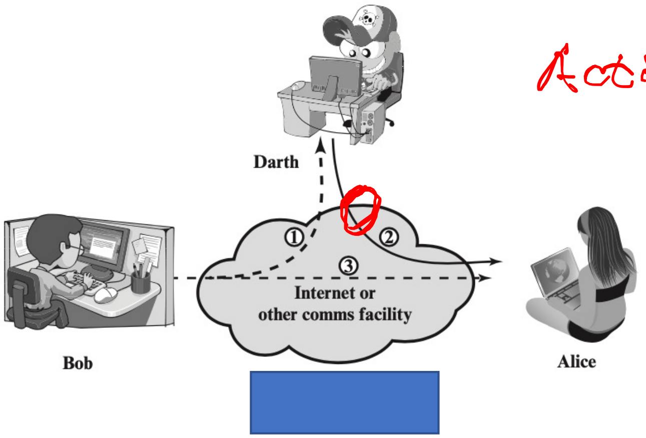
Other Security Architectures

- NIST, Cybersecurity Framework (CSF)
  - https://www.nist.gov/cyberframework ✓
  - VIRTUAL WORKSHOP #2 | February 15, 2023 (9:00 AM – 5:30 PM EST). Discuss potential significant updates to the CSF
  - https://www.nist.gov/news-events/events/2023/02/journey-nist-cybersecurity-framework-csf-20-workshop-2 pdf.
- OWASP - Open Web Application Security Project
  - Web application security
  - OWASP Application Security Verification Standard (ASVS) - https://owasp.org/www-project-application-security-verification-standard/
  - OWASP Web Security Testing - https://owasp.org/www-project-web-security-testing-guide/
  - OWASP foundation

Security attack

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





Active.

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?

Encryption,

MAC.

NIC

Scapy

-> 2 mode

eBPF -> kernel mode

tcpdump -> user space

Active attack

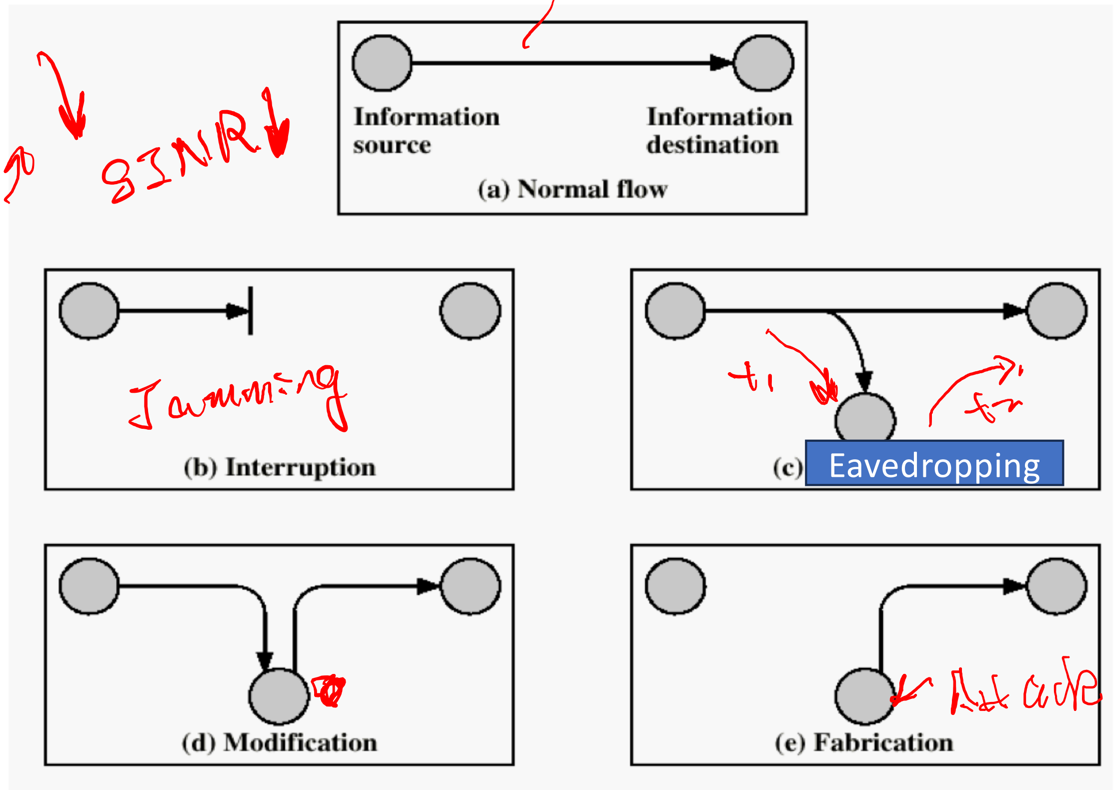
- active attack includes:
  - replay
  - Modification of messages
  - Denial of service
  - Masquerade

Example: two points communication

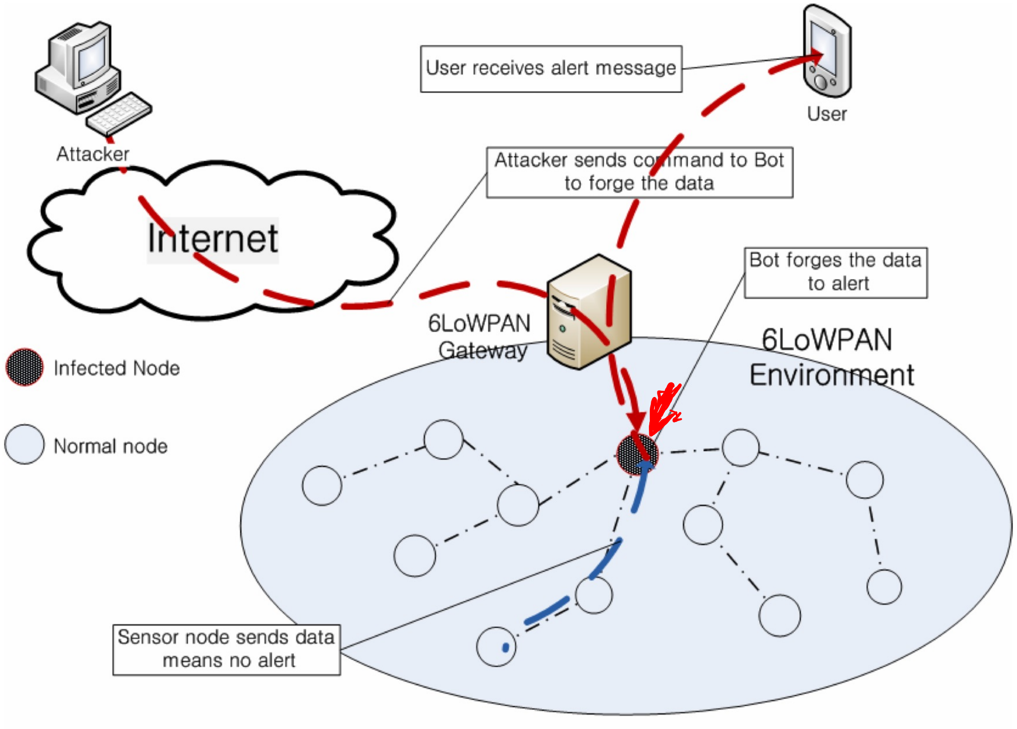
- Generic types of attacks

public

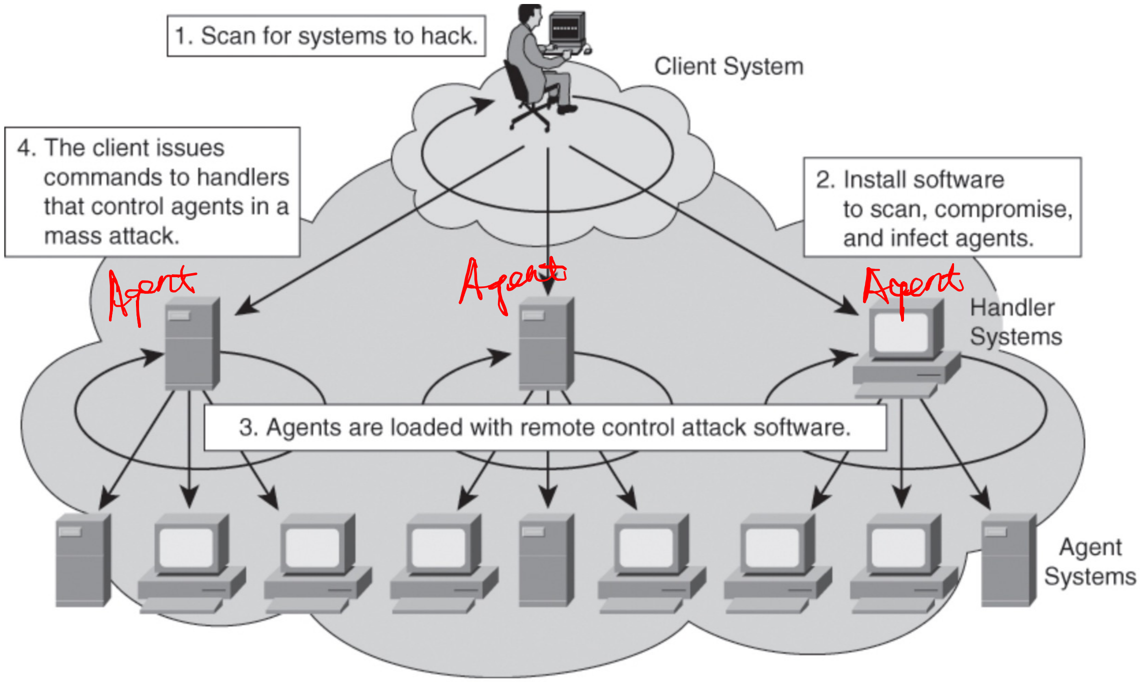
$\frac{\text{signal}}{\text{Noise}}$ ↓ SINR↓



Example of modification attack in 6LoWPAN


Attacker
User receives alert message
User
Internet
Attacker sends command to Bot to forge the data
Bot forges the data to alert
6LoWPAN Gateway
6LoWPAN Environment
Infected Node
Normal node
Sensor node sends data means no alert

Example: a group of attackers

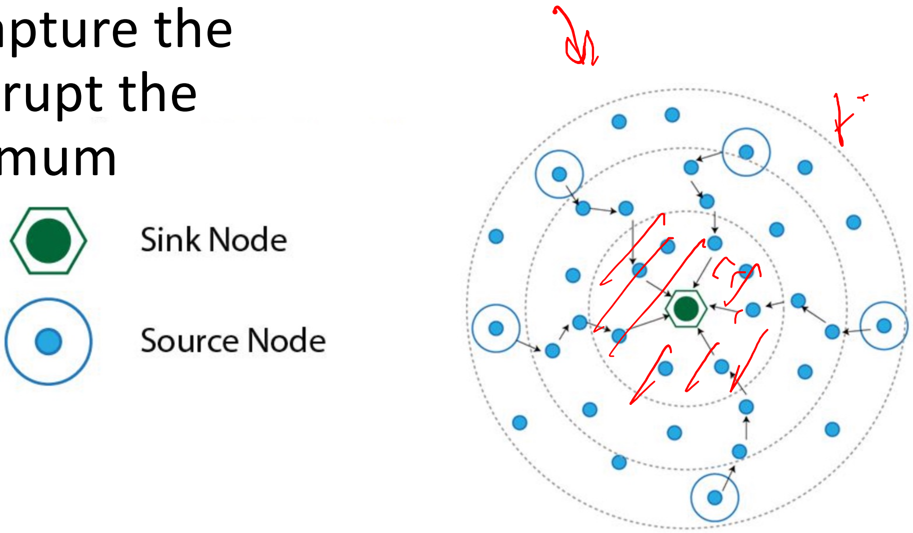

1. Scan for systems to hack.
Client System
4. The client issues commands to handlers that control agents in a mass attack.
2. Install software to scan, compromise, and infect agents.
Agent
Agents
Agent
Handler Systems
3. Agents are loaded with remote control attack software.
Agent Systems

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.”


Sink Node
Source Node