Information security

Lecture-2

Eng. Taghreed Harfoush

Vulnerability:

a weakness in a system that might be exploited to cause harm.

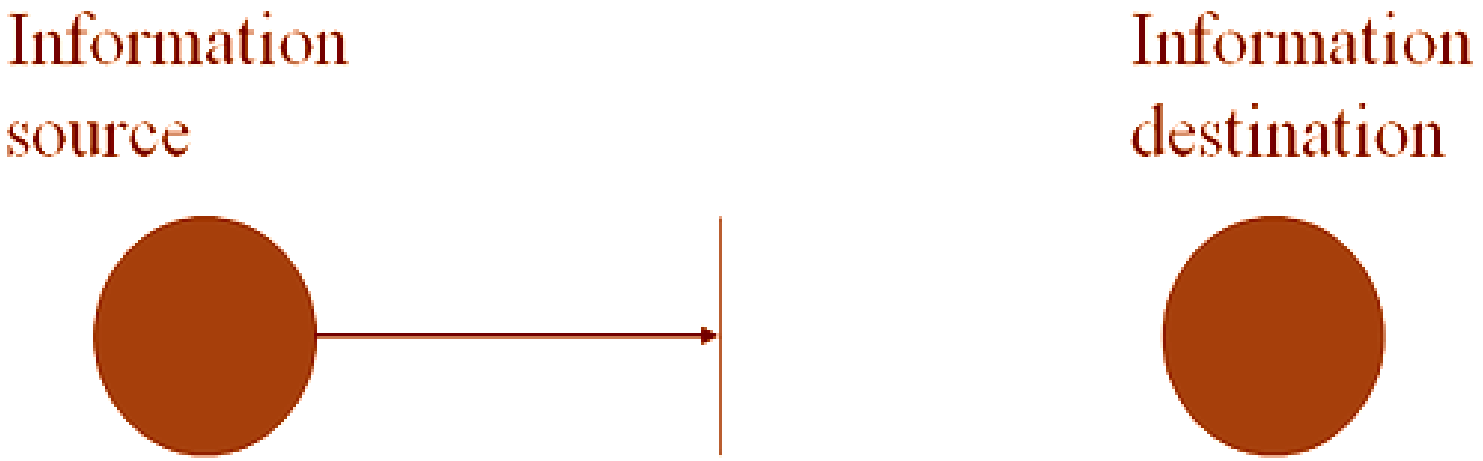
Threat

A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm. That is, a threat is a possible danger that might exploit a vulnerability.

- *Threat can be:*
  - Accidental (natural disasters, human error, …)
  - Malicious (attackers, insider fraud, …)

- أشكال التهديدات:

Interruption

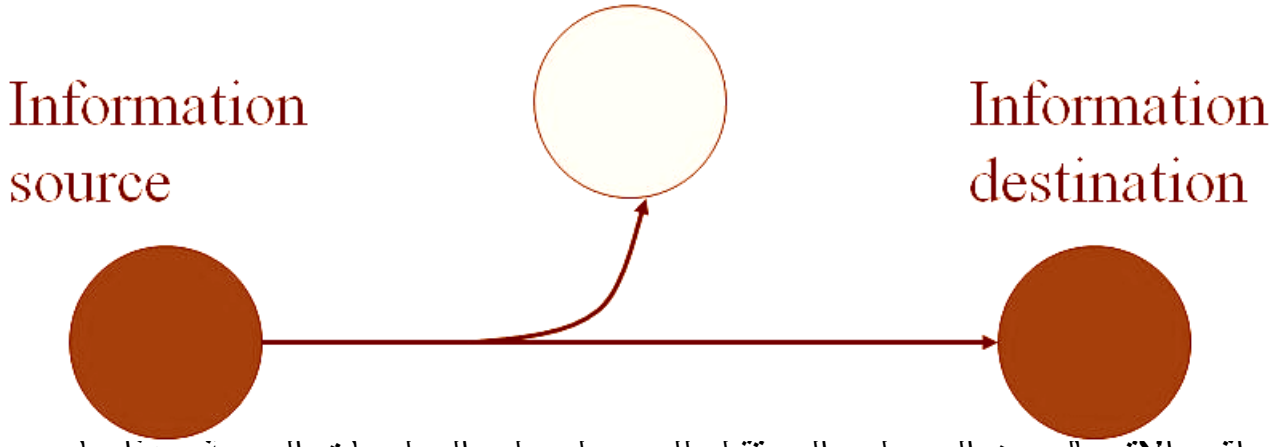


- Asset becomes lost, unavailable or unusable,
- destruction of hardware, cutting communication line, disabling file management system, etc.

- وهذا النوع يعتمد على قطع قناة الاتصال لايقاف الرسالة أو البيانات من الوصول الى المستقبل.

Interception

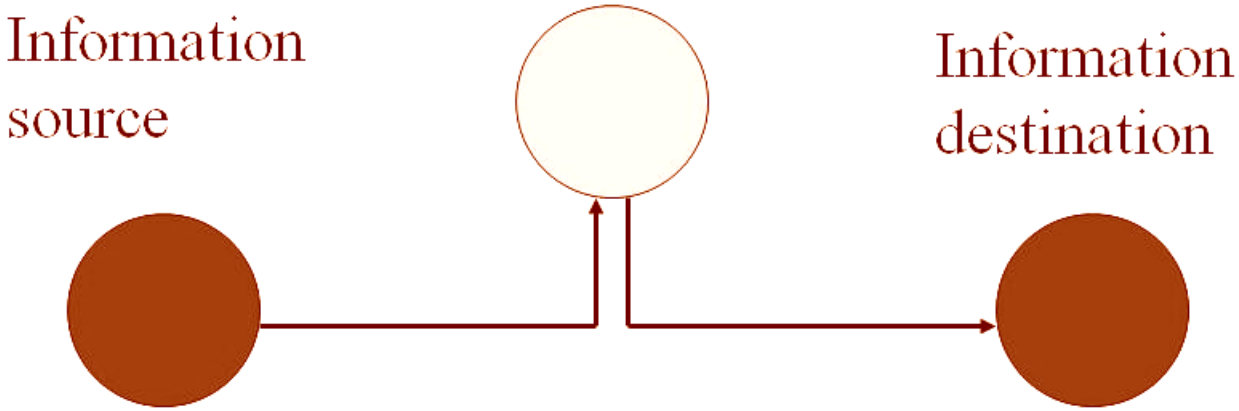
- Unauthorized party gains access to the asset
- wiretapping, unauthorized copying of files



- المهاجم يراقب الاتصال بين المرسل والمستقبل للحصول على المعلومات السرية وهذا ما يسمى بالتصنت على الاتصال. ويعتبر هذا النوع هو هجوم على السرية أو الموثوقية (Confidentiality).

Modification

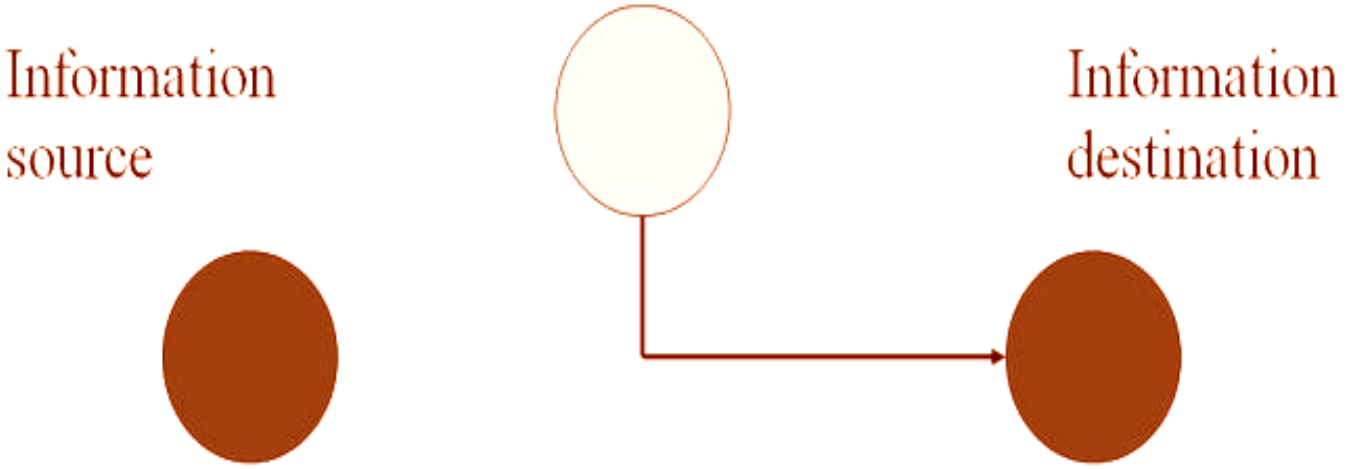
- Unauthorized party tampers with the asset
- changing values of database, altering programs, modify content of a message, etc.



- المهاجم فانه يقوم بتغيير محتوى الرسالة ومن ثم ارسالها الى المستقبل ، والمستقبل طبعاً لا يعلم بتغيير محتوى الرسالة من قبل المهاجم.

Fabrication

- Unauthorized party insets counterfeit object into the system
- insertion of offending messages, addition of records to a file, etc.



- يرسل المهاجم رسالة مفادها أنه صديقه .ويطلب منه معلومات أوكلمات سرية.

Attack:

a deliberate attempt to evade security services and violate the security policy.

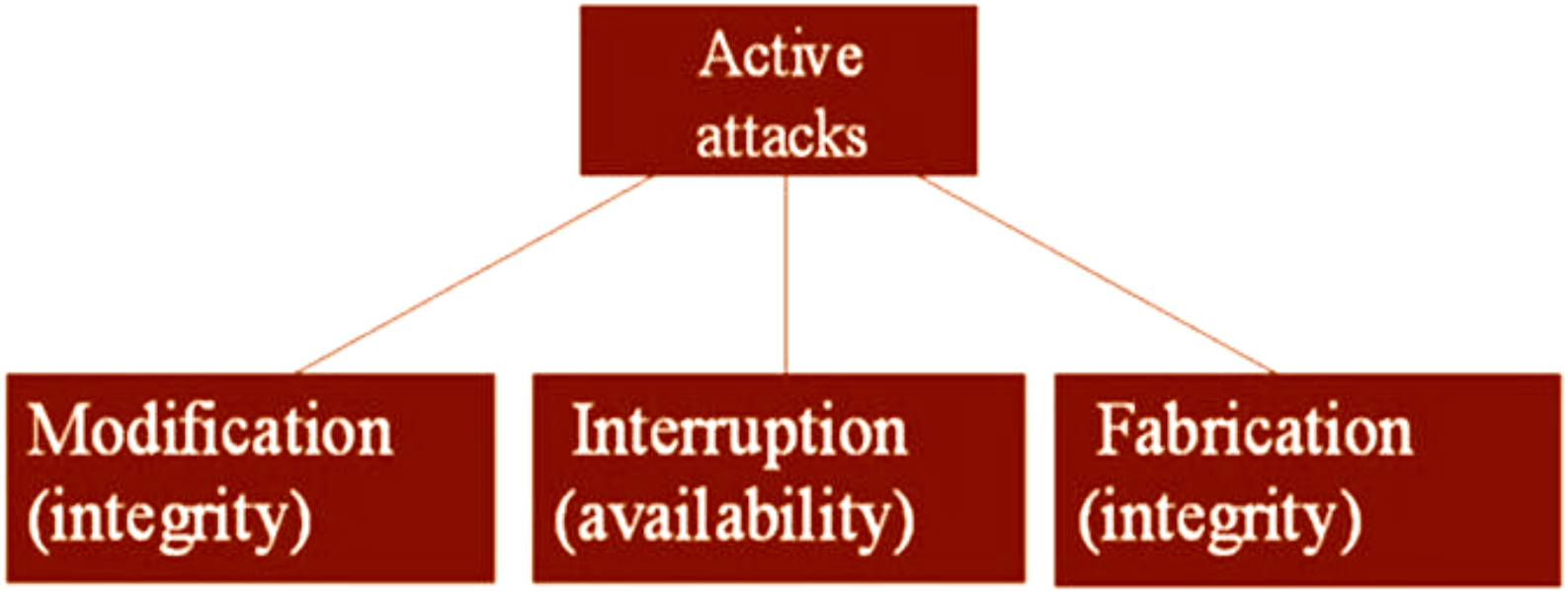
- Attacks exploit vulnerabilities

- Active attacks
- Passive attacks

- الهجمات الفعالة :
- تتطلب الهجمات الفعالة بعض التعديلات على دفقة المعطيات أو انشاء معطيات مزيفة.ويمكن تقسيمها الى أربعة أصناف : التنكر(masquerade) ،اعادة الارسال(reply)، تعديل الرسائل (modification of messege)،وانكار (رفض تقديم) الخدمة(denial of service).

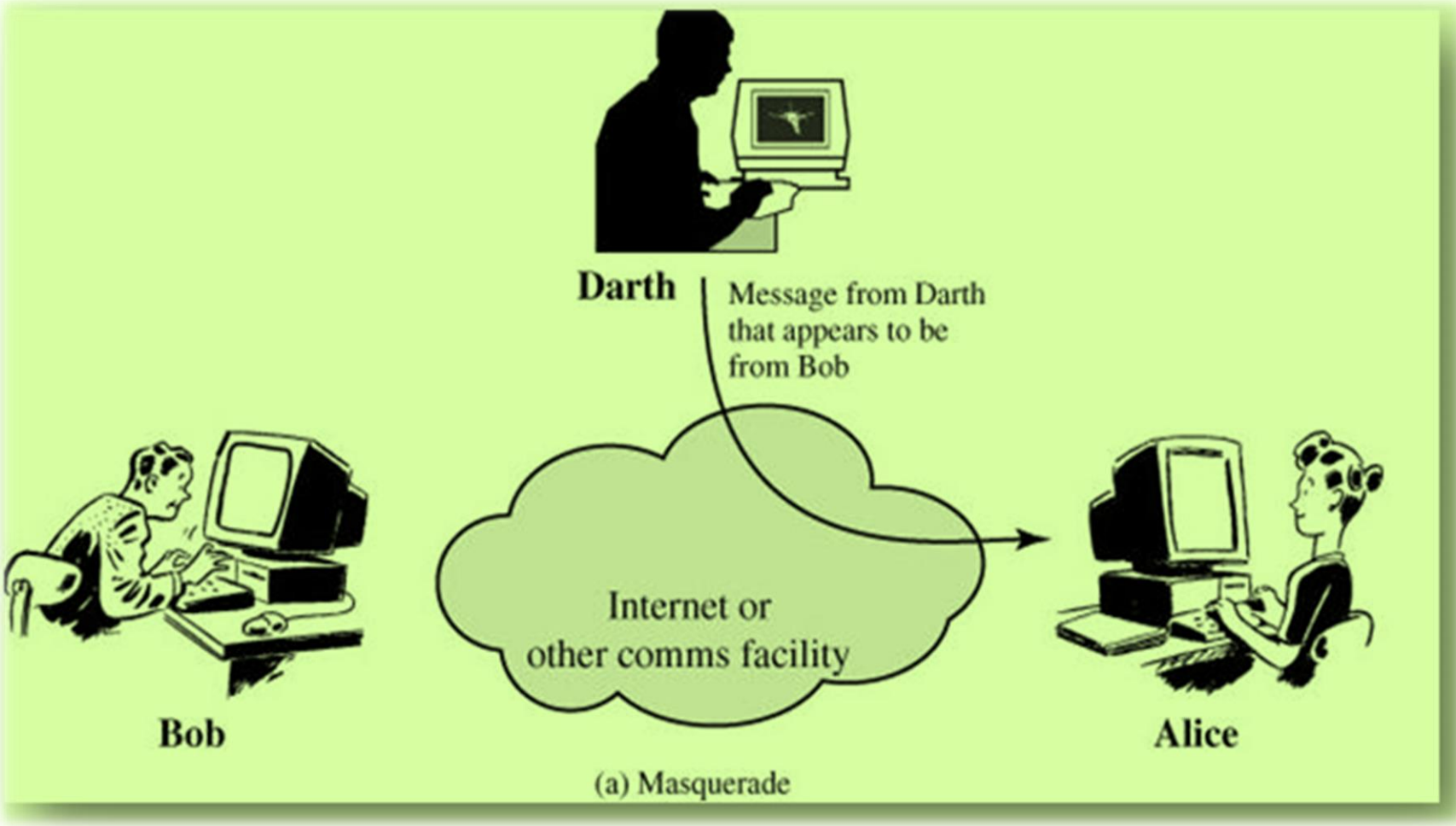
Active attacks

- An active attack attempts to alter system resources or affect their operation.

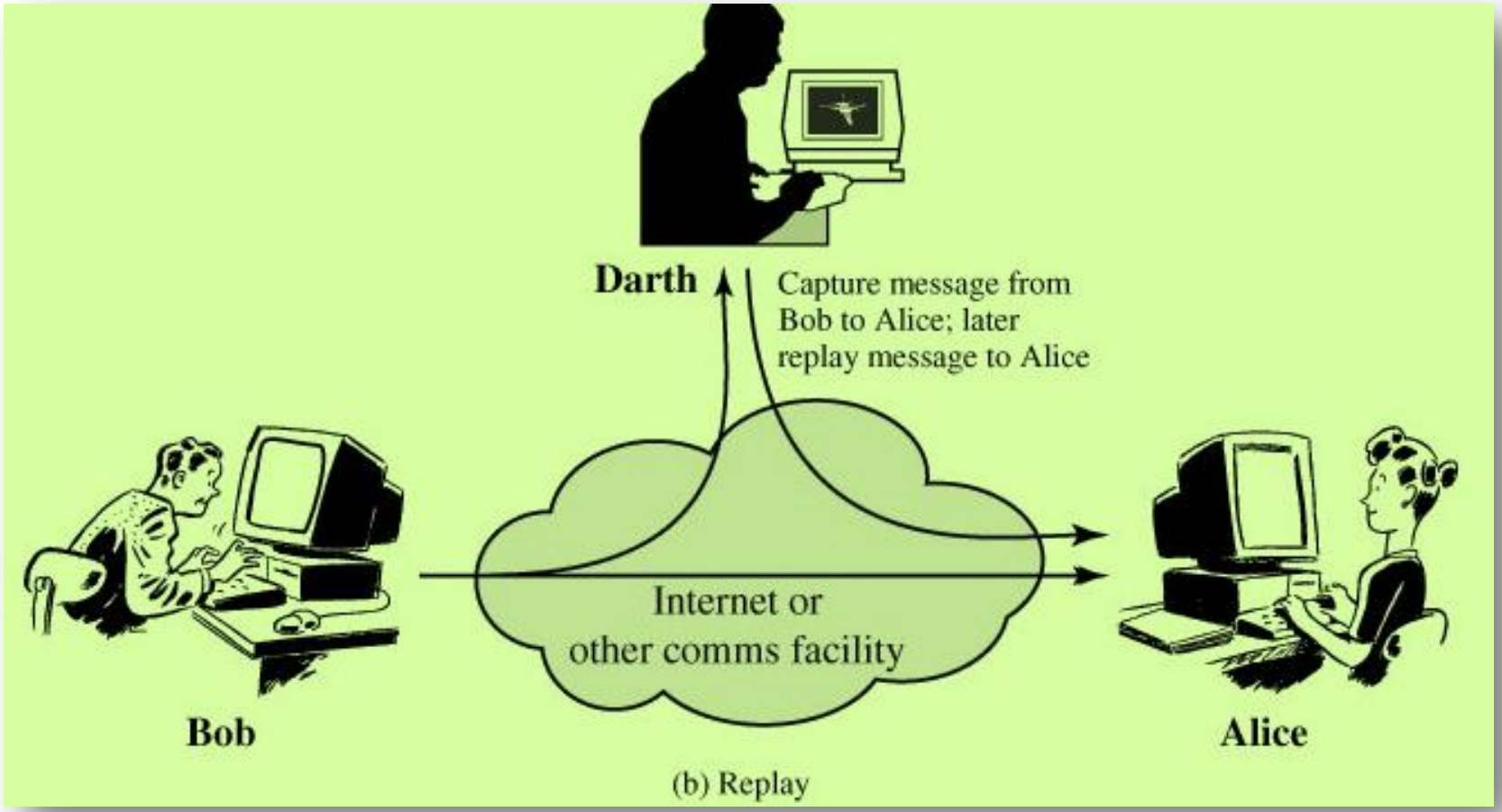


- الهجمات الفعالة :
- تتطلب الهجمات الفعالة بعض التعديلات على دفقة المعطيات أو انشاء معطيات مزيفة.ويمكن تقسيمها الى أربعة أصناف : التنكر(masquerade) ،اعادة الارسال(reply)، تعديل الرسائل (modification of messege)،وانكار (رفض تقديم) الخدمة(denial of service).

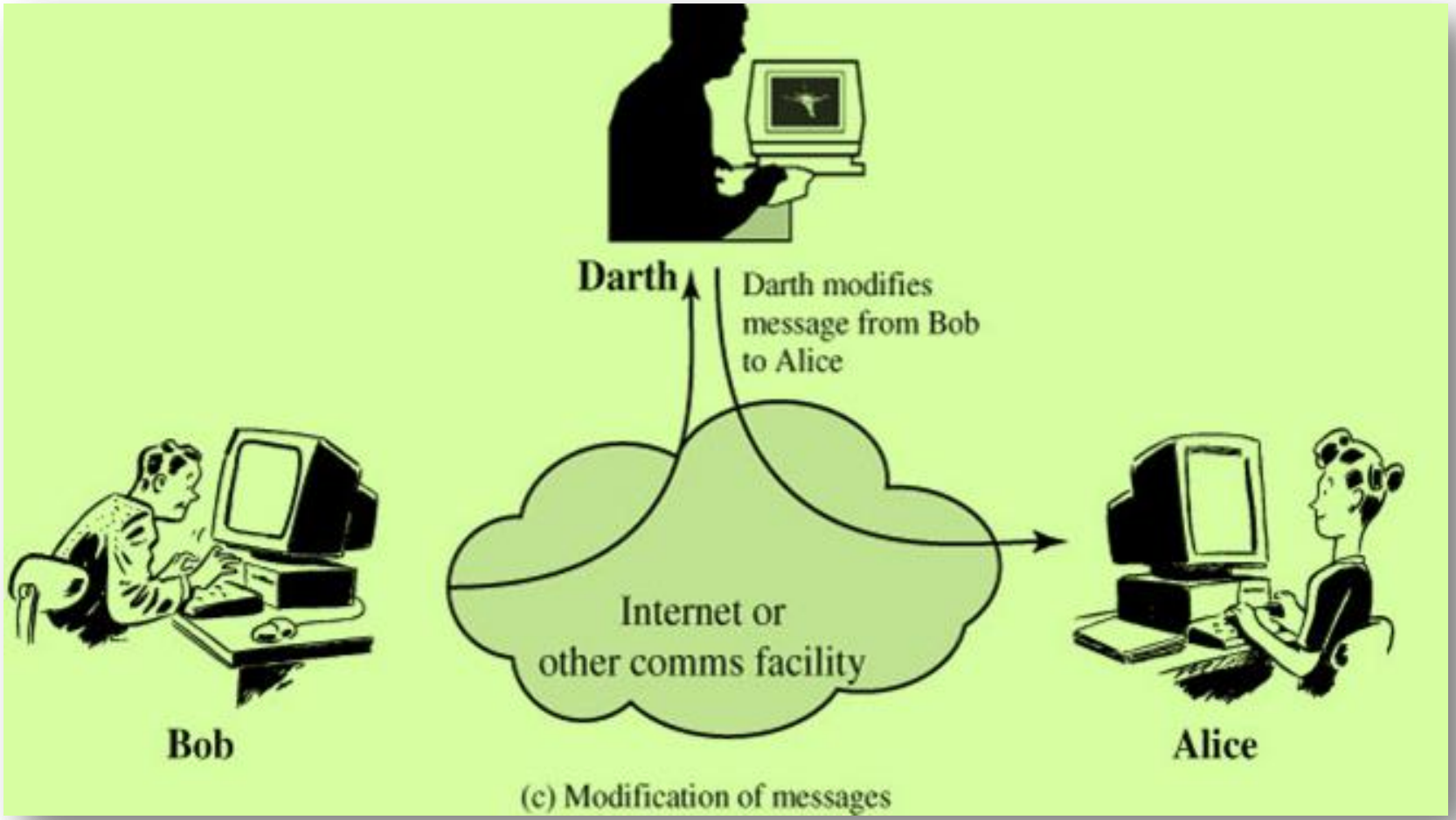
Active attacks- masquerade



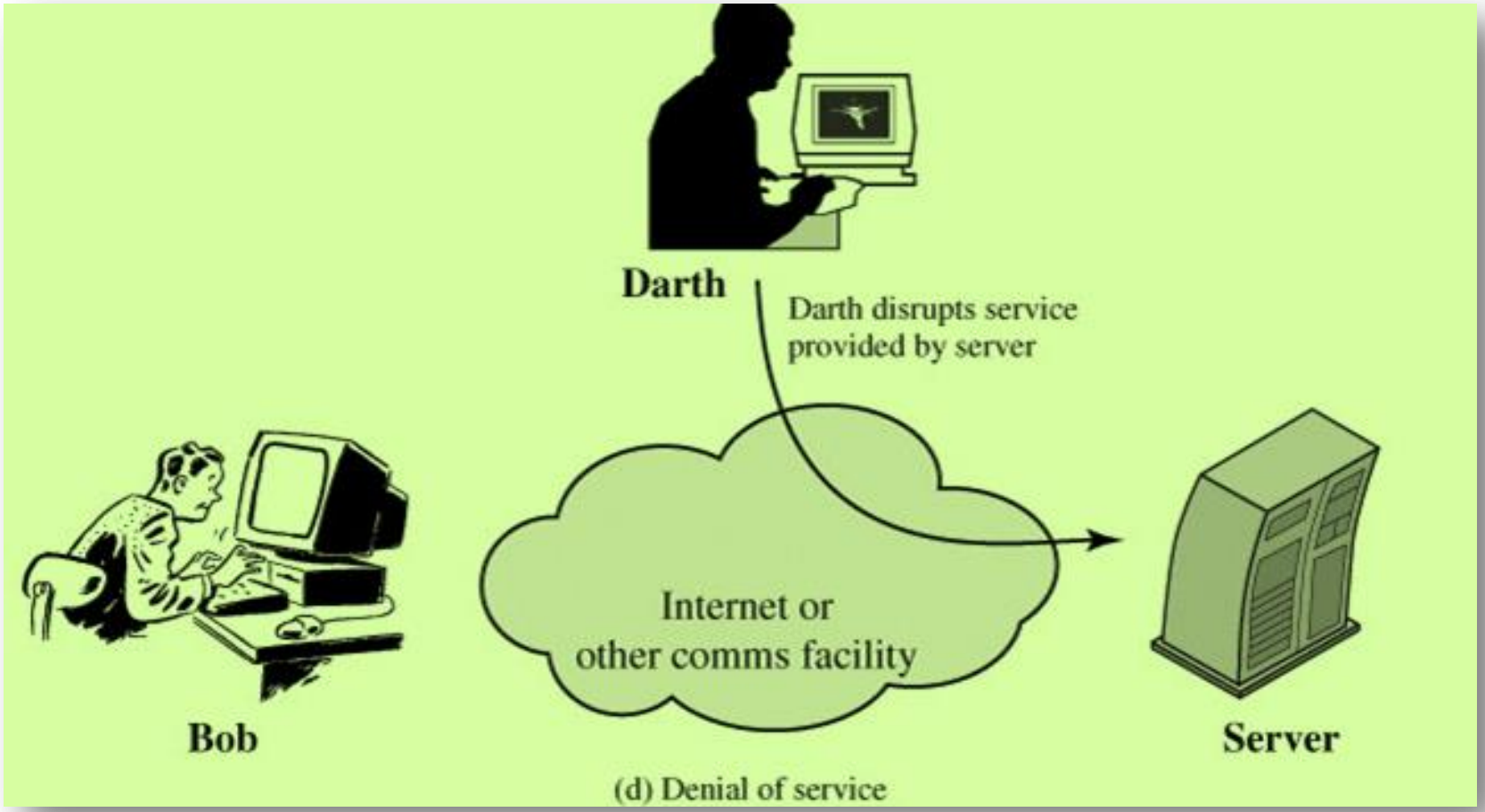
Active attacks - reply



Active attacks - modification of messege



Active attacks - denial of service

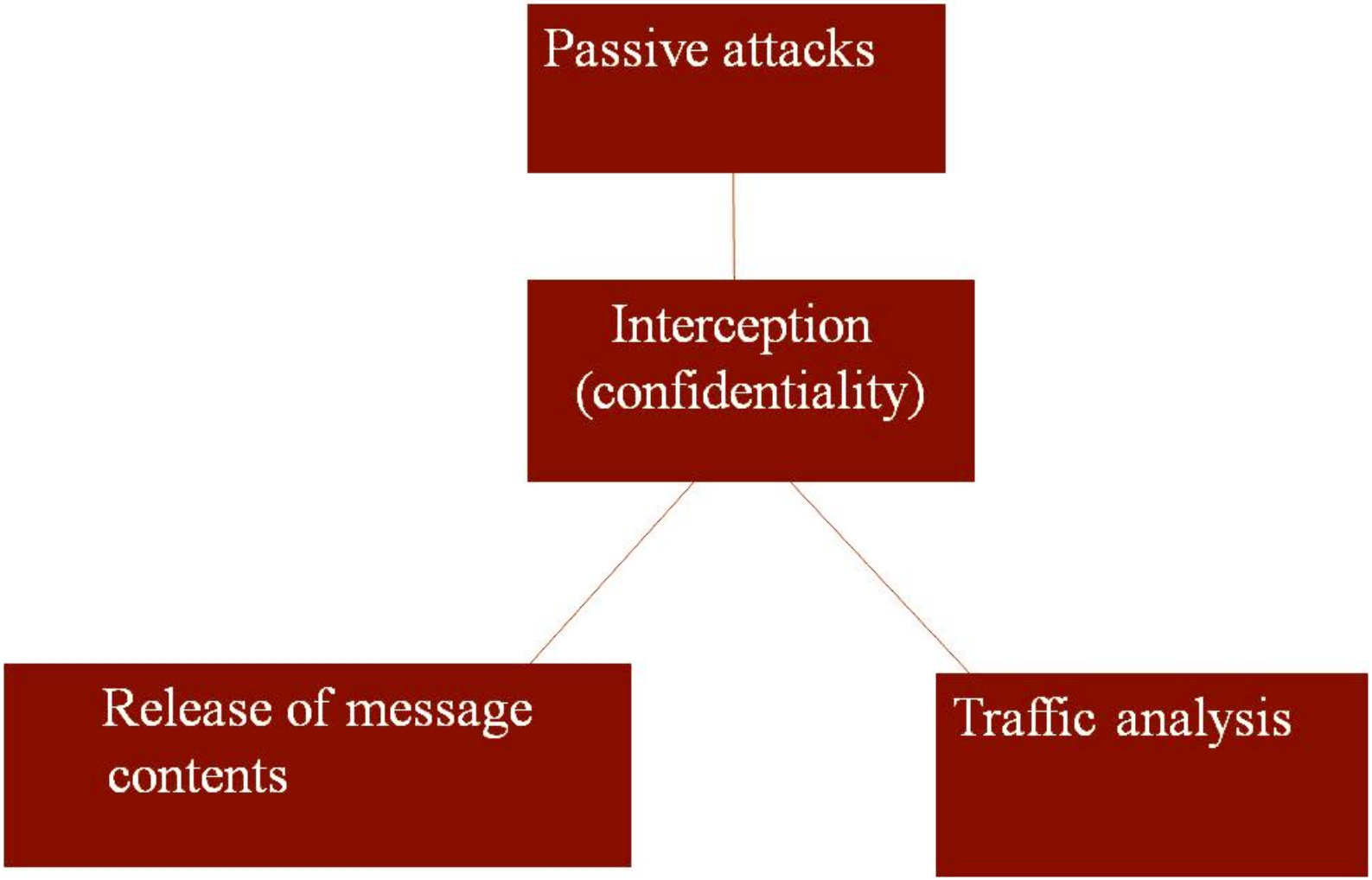


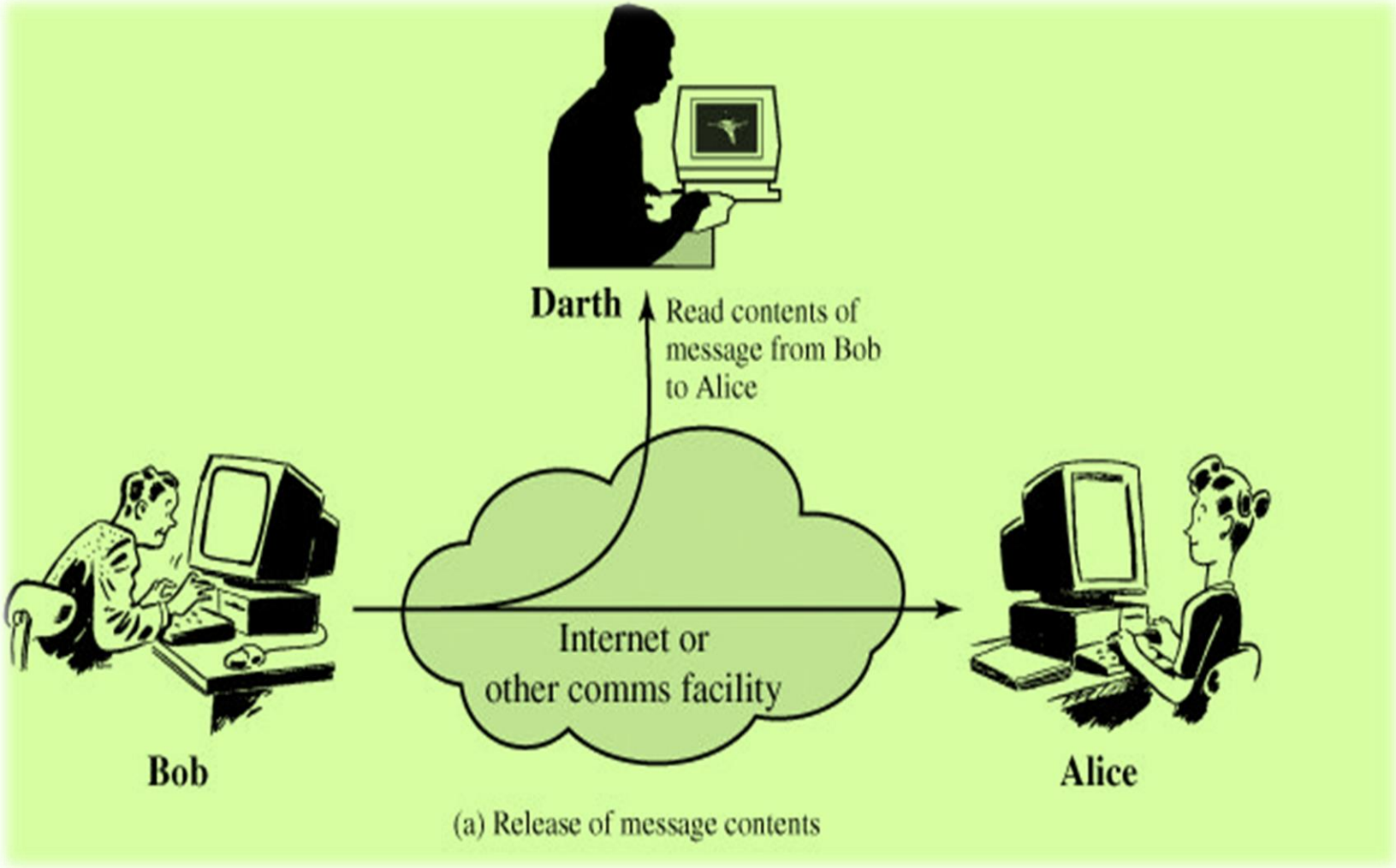
(d) Denial of service

Passive attacks

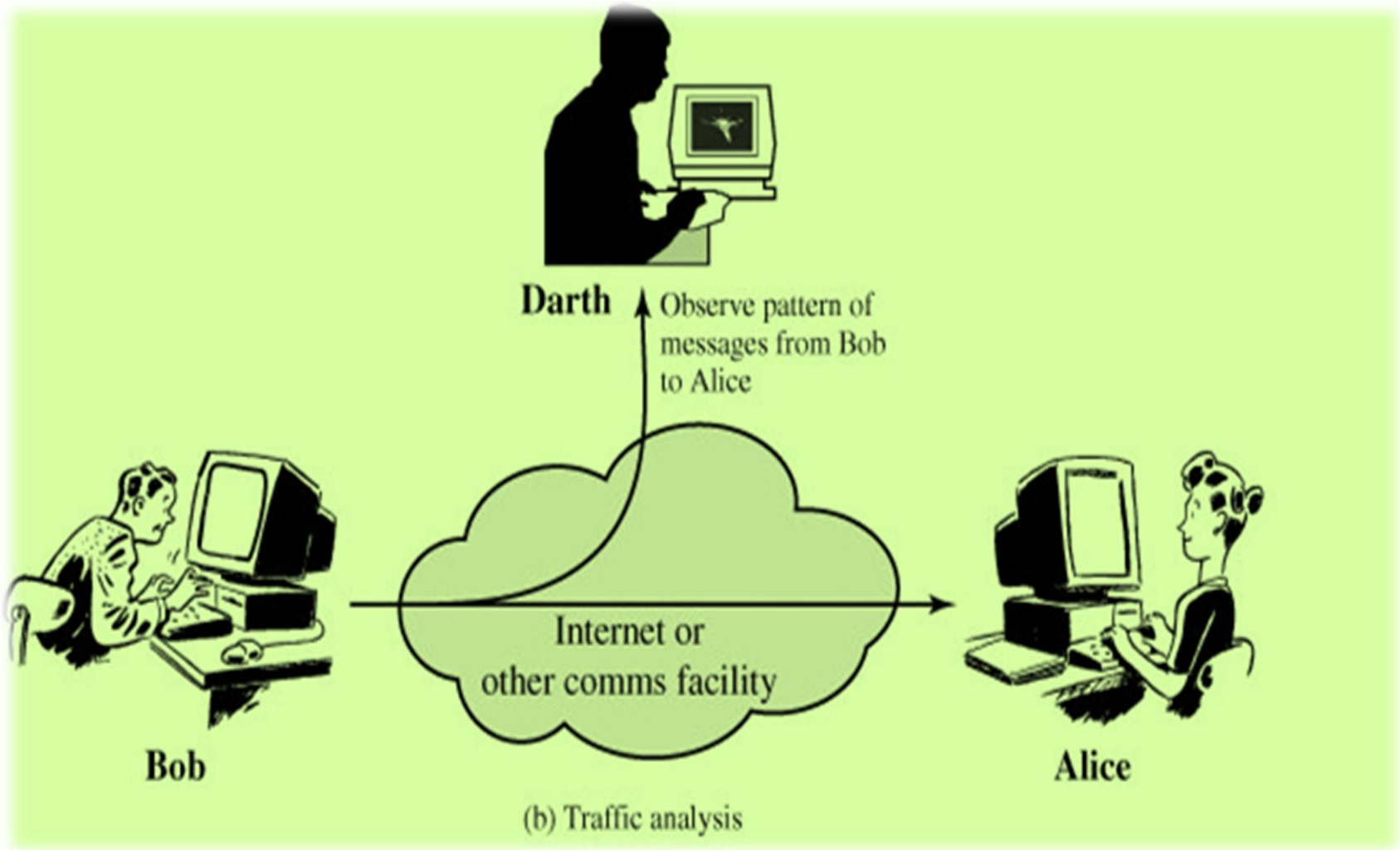
- .A passive attack attempts to learn or make use of information from the system but does not affect system resources
- Two types of passive attacks are:
  - *release of message contents*
  - *traffic analysis.*
- Passive attacks are very difficult to detect because they do not involve any alteration of the data.

- الهجمات غير الفعالة :
- من طبيعة هذه الهجمات استراق السمع ، أو مراقبة المراسلات. ويكمن هدف الخصم في الحصول على المعلومات المرسلة.
- يوجد نوعان من الهجمات غير الفعالة هما كشف محتوى الرسالة(Release of message content) وتحليل حركة السير (traffic analysis).


Passive attacks
Interception (confidentiality)
Release of message contents
Traffic analysis



(a) Release of message contents



(b) Traffic analysis

Q&A