Confidentiality, Integrity, Availability (CIA)

❑ Confidentiality

- Only those entitled to access the information can see it.
- Authorise, encrypt, access control, authenticate, restrict physical access.

❑ Integrity

- Information cannot be altered and changes are immediately detectable.
- Backup, checksum, hash, correction code

CIA

❑ Availability

- Information is available (to read, write) to those who need it without interruption or onerous access restrictions.

- Redundant systems, data recovery, disaster planning, UPS, backup power systems, redundant network connections.

- e.g. “Fail open” authentication systems have been DDOSed (loss at availability) to allow attackers to bypass access restrictions (break confidentiality)

CIA Examples

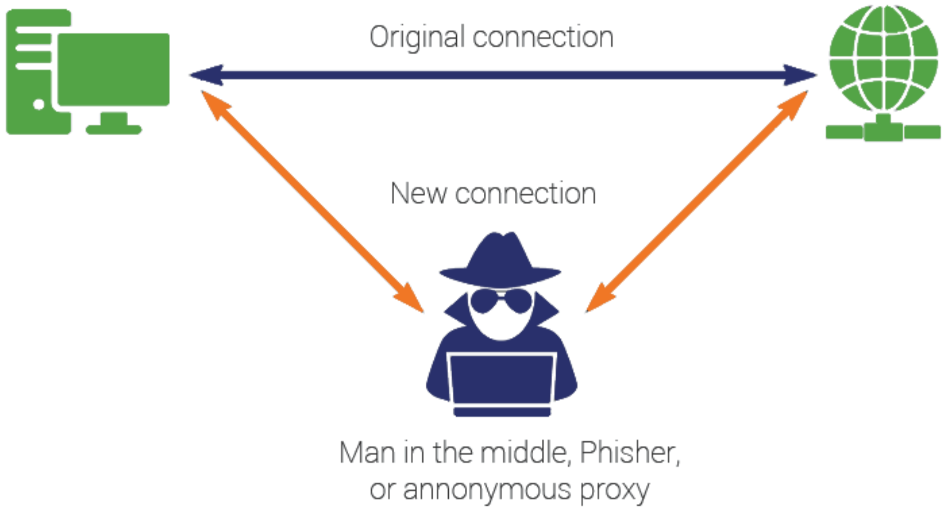

Fig 2. Man-in-the-Middle Attack

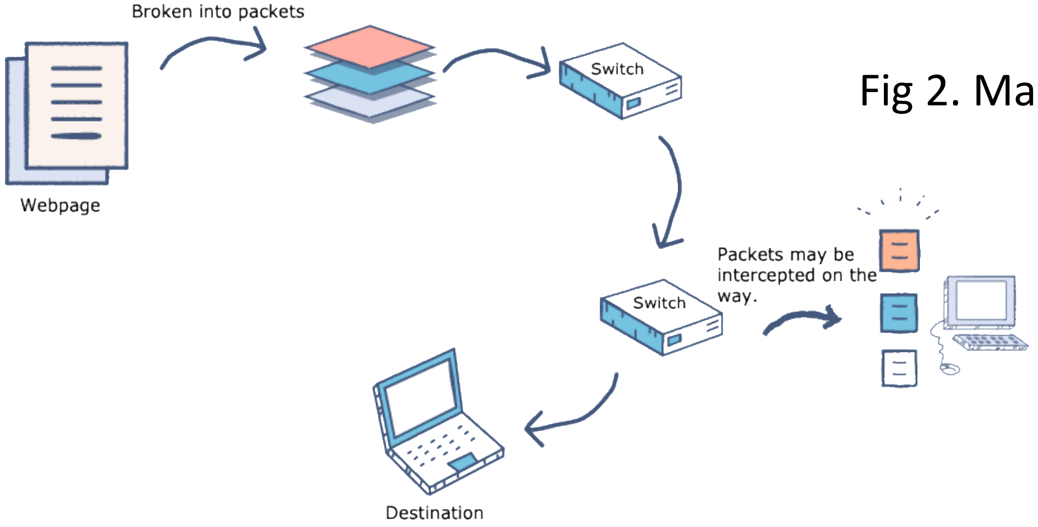

Fig 1. Packet Sniffing Attack

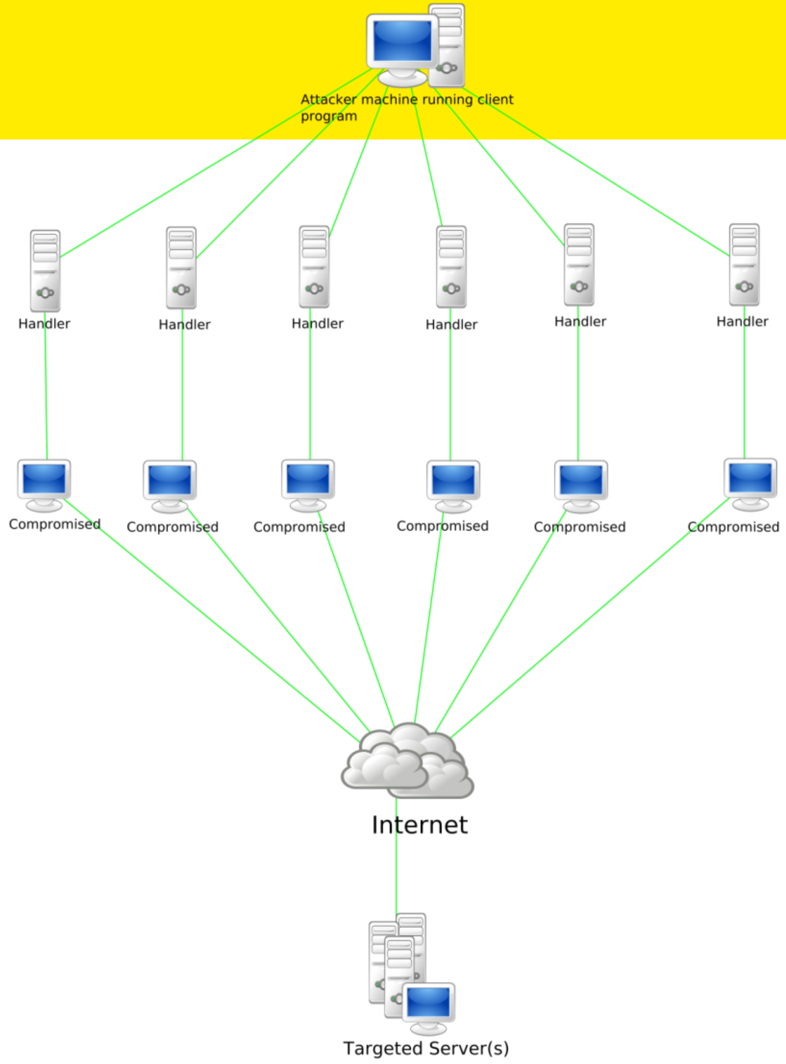

Fig 3. Denial-of-Service Attack

Trust (AAA)

❑ **Assurance**

- Ability to trust information, identity, behaviour.
- E.g. Software security assurance helps the software designed and implemented with a proper level of security.

- Certificates, SSL, authentication systems build trust.
- Phishing, pharming, spoofing, spam, erode trust.

Repudiation

❑ Authenticity

- Enforcing commitments, contracts, agreements.
- E.g. Data authenticity: digital data is authentic if it is without any successively processing.

- The internet has no fundamental way of managing this.
- Not designed for commerce, access control (paywalls) or even uploads.

Privacy

❑ Anonymity

- Internet users have an expectation of privacy, engendered by the stateless Client/Server model used for http, dns

- General Data Protection Regulation (GDPR) https://eur-lex.europa.eu/eli/reg/2016/679/oj