IP Spoofing

integrity
availability

- Routers do not validate the source
- Receiver cannot tell that the source has been spoofed

➡ An attacker can generate raw IP packets with custom IP source fields

e.g. DOS (blackhole) and MITM attacks

ICMP ping of death (before 1997)

availability

Any host receiving a 64K ICMP payload would crash or reboot

- 64K bytes payload were assumed to be invalid by programmers
- An attacker could split a 64K payload, transmit it and would be reassembled by the receiver overflowing a buffer