Network Security

Network security starts from **authenticating** the user, commonly with a username and a password. Since this requires just one thing besides the user name, i.e. the password which is something you 'know', this is sometimes termed one factor authentication. With **two factor authentication** something you 'have' is also used (e.g. a **security token** or 'dongle', an **ATM card** or your **mobile phone**), or with three factor authentication something you 'are' is also used (e.g. a **fingerprint** or **retinal scan**).

Once authenticated, a **firewall** enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as **computer worms** or **Trojans** being transmitted over the network. **Anti-virus software** or an **intrusion prevention system** (IPS) help detect and inhibit the action of such **malware**. An **anomaly-based intrusion detection system** may also monitor the network and **traffic** for unexpected (i.e. suspicious) content or behaviour and other anomalies to protect resources, e.g. from **denial of service** attacks or an employee accessing files at strange times. Individual events occurring on the network may be logged for audit purposes and for later high level analysis.

Communication between two hosts using the network could be encrypted to **maintain privacy**.

**Honeypots** essentially **decoy** network-accessible resources, could be deployed in a network as surveillance and early-warning tools. Techniques used by the attackers that attempt to compromise these decoy resources are studied during and after an attack to keep an eye on new **exploitation** techniques. Such analysis could be used to further tighten security of the actual network being protected by the honeypot.