Distributed System Models

An ***architectural model*** of a distributed system defines the way in which the components of the system interact with each other and the way in which they are mapped onto an underlying network of computers. E.g.s include the *client-server model* and the *peer process* model.

The *client-server* model can be modified by:

- The partition of data or replication at cooperating servers
- The caching of data by proxy servers and clients
- The use of mobile code and mobile agents. E.g. applets and object serialization

There is no global time in a distributed system so all communication is achieved by message passing. This is subject to delays, failures of various kinds on the networks, and security attacks. These issues are addressed by three models:

1) The interaction model deals with performance and with the difficulty in setting time limits in a distributed system, for example for message delivery.
2) The failure model attempts to give precise definitions for the various faults exhibited by processes and networks. It defines reliable communication and correct processes.
3) The security model discusses possible threats to processes and networks.

Security Model

- The security of a distributed system can be achieved by securing the processes and the channels used for their interactions and by protecting the objects (e.g. web pages, databases etc) that they encapsulate against unauthorized access.
- Protecting objects: Some objects may hold a user's private data, such as their mailbox, and other objects may hold shared data such as web pages. *Access rights* are used to specify who is allowed to perform which kind of operations (e.g. read/write/execute) on the object.
- Threats to processes (like server or client processes) include not being able to reliably determine the identity of the sender.
- Threats to communication channels include copying, altering, or injecting messages as they traverse the network and its routers. This presents a threat to the privacy and integrity of information. Another form of attack is saving copies of the message and to replay it at a later time, making it possible to reuse the message over and over again (e.g. remove a sum from a bank account).
- Encryption of messages and authentication using digital signatures is used to defeat security threats.

Problems facing designers of distributed systems

- Widely varying modes of use: The system components are subject to wide variations in workload (e.g. some web pages have millions of hits a day and some may have no hits). Some applications have special requirements for high communication bandwidth and low latency (e..g multimedia apps).

- Wide range of system environments: A distributed system must accommodate heterogeneous hardware, operating systems, and networks (e.g. wireless networks operate at a fraction of the capacity and much higher error rates than present day LANs).

- Internal problems: Non-synchronized clocks, concurrency problems, many modes of hardware and software failures involving the individual components of the system.

- External threats: Attacks on data integrity, ensuring confidentiality, denial of service.