Recall that historically computer security has been defined to encompass:

Confidentiality: (also called secrecy/privacy) who can read information;

Integrity: who can write or modify information;

Availability: are resources available when needed.

Availability Attacks

Attacks on availability are called denial of service or DoS attacks. An attacker prevents a user from accessing or utilizing available system resources.

A particular class of DoS attacks are labeled Distributed Denial of Service or DDoS attacks. These typically involve co-opting the services of many other machines to participate in the attack, a botnet.

Gresty’s Framework

David Gresty at Liverpool John Moore's University classifies DoS attacks into two groups:

- **the consumer problem**: (also called “man-in-the-middle” attack) the attacker gets logically between the client and service and somehow disrupts the communication.

- **the producer problem**: the attacker produces, offers or requests so many services that the server is overwhelmed.
**Typical Scenarios**

In a typical producer attack:
- the volume of requests may overwhelm the server.
- the transaction may involve some handshake (protocol); the attacker does not respond and the server ties up resources waiting for a response.

A classic example of the second is so-called *syn flooding*.

**TCP Handshake**

Via this three-way handshake a client establishes a TCP connection with a server.

Server receives the SYN packet, allocates space in an internal table and sends SYN/ACK back to the caller. The connection remains “half-open” until the ACK is received by the server or the connection times out.

**SYN Flooding Attack**

A *SYN Flooding* attack happens when an attacker forges the return address on a number of SYN packets. The server fills its table with these half-open connections.

All legitimate accesses are denied until the connections time-out.

**SYN Flooding Solutions**

Is the *SYN flooding problem inherent in the way TCP connections are established? How could you close the vulnerability?*

- *Increase the server’s queue size:* typically only 8 connections are allowed; could consume considerable resources.
- *Shorten the time-out period:* might disallow connections by slower clients.
- *Filter suspicious packets:* if the return address does not match the apparent source, discard the packet. May be hard to determine.
- *Change the algorithm:* instead of storing the record in the queue, send the information encrypted along with the SYN/ACK. A legitimate client will send it back with the ACK.
Availability attacks are called “denial of service” attacks.

An attacker can either block traffic from clients (the consumer problem) or flood the server (the producer problem).

Syn flooding is a classic DoS attack.

Next lecture: Availability II