Foundations of Computer Security

Lecture 72: Availability II

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin
A filter or *packet sniffer* can detect patterns of identifiers in the request stream and block messages in that pattern. *Ingress filtering* means sniffing incoming packets and discarding those with source IP addresses outside a given range (e.g., those known to be reachable via that interface).

It is a very hard problem to be able to discriminate patterns of attack from patterns of standard usage.

An overly aggressive filter also gives a type of denial of service by discarding too many legitimate requests.
A good *firewall* can help by filtering out illegal requests. However, a typical DoS flooding attack may comprise only legal requests.

An *intrusion detection system* (IDS) can analyze traffic patterns and react to anomalous patterns. However, often there is nothing apparently wrong but the volume of requests. An IDS reacts after the attack has begun.

An *intrusion prevention system* (IPS) attempts to prevent intrusions by more aggressively blocking attempted attacks. This assumes that the attacking traffic can be identified.

IDS/IPS are useful for confidentiality and integrity attacks, not just DoS attacks.
A DDoS attack comes when an attacker takes over a number of nodes in a network and uses them as bots to launch a coordinated producer attack. *How might you counter them?*

1. *over-provisioning the network*—have too many servers to be overwhelmed (expensive and unworkable);
2. *filtering attack packets*—somehow distinguish the attack packets from regular packets (may not be possible);
3. *slow down processing*—disadvantages all requestors, but perhaps disproportionally disadvantages attackers;
4. *“Speak-up” solution* (Mike Walfish)—request *additional* traffic from all requestors.

Walfish’s solution assumes that the attacker’s bots are already maxed out. So this solution raises the proportion of valid to invalid requests.
Availability attacks are difficult to counter because it is very hard to distinguish legitimate from illegitimate traffic.

Various solutions attempt to block incoming traffic or to detect anomalous activity.

Next lecture: Intrusion Detection