Denial of Service – Attacks from the Internet (2)

Attacks on company networks endanger business processes, and the number of "denial of service" (DoS) attacks is growing. The first part of this article sketched the goals and effects of DoS attacks and covered some types of attacks. In the second half, the author treats additional types of attacks and what should be done to counter these attacks from the Internet.

The first part of this article introduced the concepts of overloading resources and attacking transport protocols (http://www.sap.info/en/go/17937). Another type of DoS attack targets network services. Every network needs protocols and services to organize itself or to perform the typical network tasks. Protocols exist to determine the most effective route for a data packet from the sender to the target and to allow computers to be addressed with a name rather than a numeric address that human users would find difficult to handle. If an attacker succeeds at manipulating these protocols and services in a way that makes the information unintelligible, errors arise that lead to a DoS. A favorite technique of attacking corporate networks is to deliver data packets to the wrong address.

Attacks that detour information can use several options because several protocols direct the path of a data packet over the network. An attacker can provide the address of a computer that accepts all data packets, but never transfers them to their intended recipients. An attacker can also give an address that doesn't exist at all. In either case, a system is no longer able to communicate with other systems.

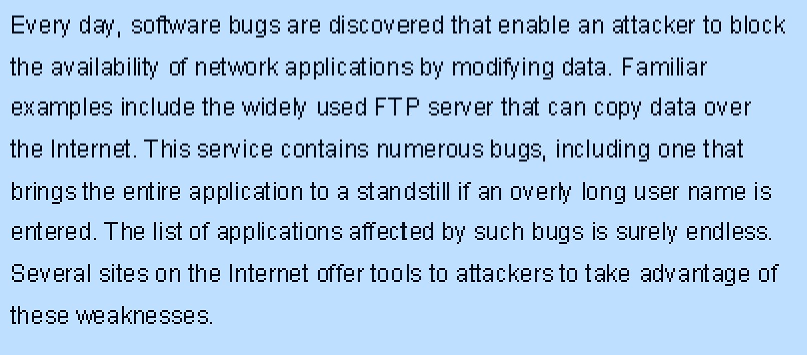
A favorite form of detour attack manipulates the network router, which transfers data packets to several networks. Since routers should transfer packets along an efficient route, they exchange information with each other so that they calculate the most effective route. An attacker who impersonates a router can send manipulated information to other routers on the network. For example, the attack might tell the network routers that then best route for a data packet is over a system that does not actually exist. As a result, all packets from that system that should go to other systems will disappear into the innards of the system. Essentially, methods exist to manipulate all the protocols used within a network to compromise communications.

Attacks on Weaknesses in Applications

Many users of Windows-based operating systems have already experienced a blue screen or a complete overload of the processor. In both cases, users can no longer work with the system until they reboot. These symptoms are only two of the possible effects of errors in applications or in components of the operating system. Yet both symptoms usualy share a common cause: an error in programming. Incorrect programming can overwrite the memory area assigned to another program, or the system might not check the data entered by a user for its content and size. The termination of a program on a workplace computer does not represent a major outage, but the crash of a network-based, multiuser application because of a programming error can terminate the application, making it impossible for anyone to work with it.

Compromised Systems with Virus Infections

Ever since the appearance of the notorious e-mail viruses I LOVE YOU and MELISSA, it's generally known that viruses can compromise systems well beyond the borders of a given corporation. In the past, weaknesses in the protocols for sending e-mail and lax security on workplace computers have combined to create an avalanche-like spread of these viruses, crippling the Internet connection of many companies. Infections by these viruses have shown that the security of e-mail client programs, Internet browsers, and desktop operating systems is sorely lacking in standard configurations, and that the required security features are often not present at all. SMTP, the protocol used for e-mail, has no mechanism to authenticate the sender, a situation that only makes it even easier to spread viruses in the mail.



Every day, software bugs are discovered that enable an attacker to block the availability of network applications by modifying data. Familiar examples include the widely used FTP server that can copy data over the Internet. This service contains numerous bugs, including one that brings the entire application to a standstill if an overly long user name is entered. The list of applications affected by such bugs is surely endless. Several sites on the Internet offer tools to attackers to take advantage of these weaknesses.

Software Bugs as Points of Attack

How Corporations Can Fight DoS Attacks

The measures that companies must take to fight against DoS attacks are just as comprehensive as the attack techniques. Only the interplay of all measures guarantees optimal protection. The mottos: "one-hundred percent security does not exist," and "every chain is only as strong as its weakest link," apply to network security in general.

Security updates have a high priority for system security. They hinder an attacker's ability to break into a system through well-known security gaps in the operating system or in applications, to take over a system successfully, or to execute a DoS attack. The risk of an attack is particularly high in the first weeks after a weakness is publicized. Accordingly, it's important to apply security updates as soon as they become available. Companies should implement processes that ensure that the parties responsible for the system learn of new updates regularly, test them thoroughly, and install them if needed.

Companies should harden all their critical systems. This process removes all unnecessary components from a system and applies system and application-specific, critical security settings. The most popular operating systems and applications offer instructions on how to perform hardening.

Securing the Routers

Companies should implement bandwidth limitations on the routers that connect to the corporate network or to online services. Limited bandwidth for access to the target system hinders an attack from a flood of data packets. The permissible bandwidth should be defined to ensure that even maximum load does not have a critical effect on the target system. However, limited bandwidth only hinders a possible crash of the target system, not a DoS attack itself.

In addition, companies should perform the strongest possible filtering on a network's external routers and allow only the connections and protocols needed for the services offered to function. Recognizably manipulated packets should be discarded directly – and it's especially important to check the permissibility not only of incoming connections, but also of connections from the corporate network to the outside.

To prevent attacks that attempt to detour data, companies should configure their systems to use static routing information. They should also use only the routing protocols that use cryptographic mechanisms to ensure that the system accepts information only from trusted systems. Corporate networks should use only switches as network components, rather than the usual hubs. And the security features of the switch should also be activated.

As much as possible, companies should set the maximum number of permissible connections for network applications such as Web servers and e-applications. They should also perform a load test before going live with their system. The load test can simulate DoS attacks and log the results.

Companies can counter DoS attacks based upon the spread of a virus by checking all incoming and outgoing network data for viruses. A proven technique installs anti-virus software not only on each workplace computer, but also on the central gateways and proxy systems, across which all data usually flows. The database of viruses must be updated to the latest level at regular intervals. Only an up-to-date database offers protection against new viruses. Security for the operating systems and applications (such as Internet browsers and e-mail clients) installed on workplace computers is also important to limit attacks by viruses and by the spread of viruses. In addition to preventive measures that help limit DoS attacks up front, additional procedures must be developed to recognize and deal with DoS attacks.

The Threat Is Real and Always Changes

IT security is a living organism. The techniques used for DoS attacks continue to develop; the methods and procedures involved change almost daily. And the countermeasures must be just as dynamic and adaptable. A formal IT security policy does so best: it should form the cornerstone of all security within a corporation.

Author: Oliver Karow - Oliver@greyhat.de