

# Securing Networked Computers

The role of a computer network should, in its simplest terms, be to carry commands and information from client software running on one computer to server software running on another computer, and to return information in response to those commands. Servers can be divided into two types: those that are freely available to any client and those where access is restricted by some test such as a password, a certificate or an IP address. In an ideal world this would be all the security that was needed: however, this ideal fails in reality for two reasons.

## Unnecessary services

The vast majority of computers run far more network server programs than they need to. In the name of ease-of-use, even basic workstations will often be configured to run web, mail and DNS servers that are wholly unnecessary. In most cases the users and owners of these computers will be unaware that these services are even present. In the case of public services, these may well give out unintended or incorrect information. If the owner does not know a service is present, there is no reason for them to configure it correctly. In the case of restricted services the problem may well be worse, as an unconfigured service will either require no authentication or, at best, the same authentication as every other unconfigured machine of that type. In either case, the service is likely to be accessible to intruders, giving them unintended access to, and partial control of, the computer.

## Imperfect services

All services, even well-maintained, intentionally-run services, are provided by computer programs, some of them very complex. The complexity of these programs means that they are extremely unlikely to be perfect: they will contain bugs.

Most of those bugs will cause the service simply to fail in some circumstances. Attempts to provoke this type of failure are known as denial of service attacks. However a more dangerous type of failure is one that allows an external command to invoke some function on the server computer that was not supposed to be available. For example, a bug in a restricted server could allow a service to be requested before the necessary authentication has been performed; even more seriously, a bug in either class of server might allow commands to be given to the host computer that were not supposed to be part of the service at all.

In the worst case, a bug may result in part of the external input being executed by the host computer's command interpreter. This allows the intruder to run any operating system command they wish, to read or modify information, or alter the configuration or operation of the computer itself. Many services require special privileges to operate normally, and an intruder will often be able to inherit these privileges. This will often give the intruder the same powers as the all-powerful administrator. A computer where this type of bug has been exploited, where an external user is able to run commands as if they were the authorised administrator, is no longer under the control of its rightful owner. With some understatement it is said to be compromised.

# Reducing the impact

The impact of these problems can be reduced, and this is best done by a combination of the three different approaches described below.

## Reduce service numbers

Removing unnecessary services reduces the number of targets available for the intruder to attack. This can be done relatively easily as part of the installation process for each computer; however continued monitoring is then needed to ensure that services are not added or re-enabled accidentally during the life of the system.

## Secure remaining services

Those services that are needed, and especially those that must be provided to external and untrusted networks, must be kept in as secure a state possible. It may be possible to remove some features by initial configuration; thereafter it is essential to act promptly when security notices are issued by the software vendor and other trusted sources. These may recommend software updates or amendments, usually in the form of patches, or changes to the way services are used. The source of such recommendations should always be checked before acting on them, because unfortunately it is common for malicious advice or programs to be distributed claiming to be security improvements. If the severity of the problem permits a short delay, any changes should be tested on a non-production system first.

## Restrict access

Removing and patching services can only protect those systems where the services are known to be running. To protect other systems where services should not be needed but may be run by accident, it is necessary to configure routers or firewalls to restrict the network traffic that can reach them from other networks. For example there should be no need to run servers in public workstation rooms so potentially hostile requests should be blocked from reaching that sub-network. Since it is normally much easier to list the services that should be present, the best way to configure a router or firewall is to permit only traffic for those services and deny all others. This default-deny approach also gives the best chance of protection against unknown future threats.

## Conclusion

Removing unnecessary services, patching necessary ones, and installing router and firewall controls cannot remove the risk that computers will be compromised, but will very substantially reduce it. The vast majority of incidents reported to Computer Emergency Response Teams could have been prevented if these steps had been taken.

## References

The security of networked computers is addressed in much more detail in our Technical Guides:

*Security Matters,*

GD/JANET/TECH/001

<http://www.ja.net/services/publications/technical-guides/tg-security.pdf>

*Firewall Implementation at JANET-connected Organisations*

GD/JANET/TECH/015

<http://www.ja.net/services/publications/technical-guides/firewall-implementation.pdf>

Detailed information is available from the JANET-CERT website:

<http://www.ja.net/CERT/>