



Hidden Threats: Internal Server Vulnerabilities

How vulnerabilities on internal networks can be exploited from afar

Jürgen Pabel, CISSP

Computer systems that operate in “internal” environments often lack up-to-date security patches, despite all best practice recommendations. The risk of abuse by users with access to these networks are sometimes even recognized and accepted by the network operators, but some technologies may allow the exploitation of vulnerabilities across network and security borders.

Web servers now host many applications used within the internal environment, but they can be used as attack vectors for internal networks from external sources – be it the Internet or any connected Extranets. Attackers with knowledge about the logical location of vulnerable web applications might be able to induce the user's browser to deliver malicious content to the vulnerable server and thus gain control over the execution environment. Just how would potential attackers gain knowledge of such information? Your user's web browsers may actually be providing them with that information: the HTTP standard defines a field (“Referer:” - yes, it is in fact misspelled in the standard) which allows clients to provide the web server with additional context information in order to provide customized content. Every visited web server now becomes a potential threat to your internal network security if this server is under control of a malicious party and if it is actively evaluating the provided referrer information for potential attack targets. By delivering specially crafted, but technically valid, content to the web client it can instruct the client send malicious content to the vulnerable server and thus compromise its security.

Email servers and most integrated mail processing applications like virus scanners and SPAM filters also commonly provide detailed information which can be used to determine their vulnerability status. Certain attacks may than be possible, even if they operate behind a properly secured mail server and can not be directly addressed by attackers.

While these attacks are technically challenging and only applicable in a limited number of scenarios, it's nevertheless a risk demanding attention. Fortunately, it's technically easy to implement filters for specific information about internal systems at the network borders. However, this precaution only ensures that this sensible information is not being leaked, it does not actually protect those vulnerable systems from such attacks – the only solution is to maintain the security of every system.