Axioms of computer and network security
DRAFT

Jeffrey S. Marker, CISSP
magic@jiffyscript.com

March 27, 2002

The world is full of bad people.

1 User supplied data

User supplied data can not be trusted. It has never been trustworthy, and it shall never be trustworthy. The only data that can ever even remotely warrant trust is system supplied data, and even that should be viewed with suspicion.

This may be the most important and the most commonly forgotten axiom in all of security. Failure to recall this axiom has lead to security hole after security hole, many of which are easily exploitable. Time after time, advisories have been issued regarding commonly used "cgi" programs on the World Wide Web. Invariably, the problem arises because the people writing the programs believe either that the users will either always have good intentions or not know how to exploit the hole.

User supplied data is found in many forms. Possibly the most common in modern times are the headers in electronic mail and on USENET news posts. Netscape's mailer, for example, requires the user to enter her/his email address before s/he can send mail for the first time. The contents of that field are used both as the "From" field for the outbound mail and, partially, as the hostname used in the HELO message to the remote mail server. Unfortunately, these two forms of itentification are often used as the destination for complaints regarding unsolicited bulk email and USENET

spam. Clearly, it is not only programmers who mistakenly trust user supplied data.

2 Bound Checking

When programmers write programs which are indended to be used, they invariably end up using variables with finite boundaries. Unfortunately, they often fail to make certain that these boundaries are not exceeded. This, in turn, often leaves the door open for a user overflow these boundaries. Generally, this poses no danger, because users generally are not malicious. However, there will always be the user who is an exception to the rule. Such a user often can carefully craft input (see User Supplied Data) which will overflow the buffer and lead to arbitrary execution of commands.

In general, it is most benificial for the maluser to be able to overflow the boundaries of variables in programs which will be run with many privileges (for example, uid 0 on UNIX systems.)

3 Viri

A couple of times a year, the media will begin to run stories intended to warn the public of the upcoming due date for some computer virus. Another few times, companies will send notice to their employees, again warning of a virus. These warnings are, by and large, well indended but bogus. Viri are not the concern they once were, mainly because they can so easily be avoided, detected, and disinfected. Sound backup practices will make viri insignificant. Detection and disinfection are easily accomplished with any one of a number of products on the market, as well as a number of free and/or shareware products. Additionally, not using machines with no memory boundaries will make viri much less common.

4 Trust relationships

Trusting the non-trustworthy is bad. Determining who is not trustworthy is hard.