The Legion Security Philosophy

While Legion itself will be subject to a number of different design constraints, documented elsewhere, there are a number of concerns specific to security that influence any solution to the problem. Here then is a very brief outline of the Legion security philosophy.

Do No Harm

Legion's first responsibility will be to minimize the possibility that it will provide an avenue via which an intruder can do mischief to a remote system. Potential users must be assured that they will not come to harm from using Legion. Without such assurances, we cannot in good conscience recruit users to run Legion on their systems.

Caveat Emptor

Let the buyer beware. Legion offers tremendous computing potential, but not without some degree of risk. If a given computation is so sensitive that absolute guarantees of security are required, then it should not be performed using Legion. It is a fundamental trusth that any time a machine is made accessible to the outside world, there is a risk that security will be compromised. The best we as Legion designers can do is to minimize that risk and be as precise as possible about assessing the extent of that risk. Ultimately, the user must decide whether the benefits of using Legion outweigh the costs. But in order to make such a decision accurately, it is our responsibility to provide users with accurate measures of what those costs and benefits are.

Other Principles

- Defense in Depth
  There are no guarantees of security. Any defensive measure can be defeated. Rather than rely on any single defensive measure to provide security, a collection of independent defensive measures will be employed. The possibility and cost of defeating them all is at least as low as the possibility of defeating any one, and most likely considerably more.
- Minimize Functionality
  The larger that Legion itself becomes, and the more that users rely on Legion to enforce security, the larger the front that must be defended becomes. The more Legion code that must be trusted, the more likely a security flaw will be found in that code. Thus, we make every effort to reduce the size of Legion itself to the bare necessities
- Least Privilege
  A major flaw in many existing systems has been brittleness. In Unix, for example, if the system root is compromised, all security evaporates. Legion security will be compartmentalized, with any operation being given only the minimum privileges required, so as to avoid this problem. In particular, there will be no Legion-wide security administrator.
- Deterrence

Previous attempts at ensuring computer security have focused on preventing intrusions. Outside the electronic realm, however, the majority of laws are not enforced by prevention, but by the threat of detection and punishment. While Legion may not be able to stop all intrusions, it can detect many of them and can make it almost impossible to know when one is being observed.

legion@Virginia.edu
http://www.cs.virginia.edu/~legion/