Why Conventional Models Won’t Work

Conventional Models

Conventional security models are founded on the notion of a trusted computing base (TCB). The TCB provides a virtual machine interface that enforces a system-wide security policy. For example, it may prevent users from accessing other users’ files. Or it may only permit certain programs direct access to physical devices. The trusted computing base approach works because users can only access the sensitive objects through the interface prescribed by the system. Furthermore, the TCB is able to define a single security policy that is appropriate to all its users.

Physical Security

Legion users cannot make any assumptions about the physical security of any machine that they do not personally oversee. In order for Legion to be most useful, computations will be distributed to many more machines than any given user has control over. As a result, for most purposes, a user cannot make any assumptions of physical security. Likewise, since Legion will have no restrictions on membership, there are no assurances that any given site is not actually malicious. Finally, the networks on which Legion will execute are themselves open access and the protocols published. For all these reasons, any security "shell" that depends on physically limiting access will fail in the Legion environment.

Problems of Scale

Because Legion is intended to be scaleable to an arbitrary degree, many schemes that rely on centralized information must be discarded or amended. In particular, key generation cannot be centralized, as any central authority would conceivably be swamped by requests and become a bottleneck to performance.

Host Operating Systems

One of the constraints of the Legion design is that it must run on top of existing host operating systems. This has two serious security ramifications. The first is that any security flaws that exist in the host system will also exist in the Legion implementation residing on it. In particular, a remotely-executed Legion object, like any other user-level program, could conceivably be used to exploit such flaws. The second is that as a user-level process, the Legion system is itself vulnerable to system-level attacks. Thus any Legion host might be compromised by either a malicious operator, or by any other program that has compromised system security.

No Single Policy

Every user or group of users of Legion will have their own definition of what it means for Legion to be secure. While some sites may be primarily interested in privacy of their data, another may be concerned only with its integrity. It is neither possible nor appropriate for us as designers to dictate a single system-wide definition of security. Rather, we can only provide the mechanisms whereby users can implement their own policies. In this respect Legion differs from those systems that have been designed with a single domain and a single security policy in mind.

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