Cryptographic Techniques for Protecting Storage

Stephen T. Kent
Bolt Beranek and Newman Inc.
Cambridge, MA 02238

This presentation explores cryptographic techniques for protecting information (programs or data) stored at various levels in a memory hierarchy, i.e., archival storage, secondary memory or primary memory. The system designs described here are based on the use of tamper-resistant modules (TRMs) to protect a small amount of hardware, e.g., that containing cryptographic keys, in conjunction with cryptographic techniques for protecting physically unsecured storage. A TRM provides physical security, i.e., while the TRM is intact it prevents the release or modification of information contained within and breaking into a TRM results in destruction (erasure) of the sensitive information inside. Packaging all of the sensitive components of a computer system (processor and storage) in a single TRM is often impractical, but selected portions of a system can be protected effectively in this fashion. Cryptographic techniques are applied to all storage outside of the TRM boundary to prevent release of and to detect all forms of modification of the encrypted information. The protection against release must be thorough, e.g., no plaintext data-patterns must be visible, either at different locations in storage or at the same location over time. The detection of modification must ensure that a returned data object is the last, valid object written at the specified location and that it is intact. The cryptographic mechanisms used to provide this protection must not significantly degrade performance nor substantially increase storage requirements.

This presentation is taken from the author's doctoral dissertation, "Protecting Externally Supplied Software in Small Computers," and is available as MIT/LCS/TR-255.