Conduit Cascades and Secure Synchronization

Simon N. Foley,
Department of Computer Science,
University College, Cork, Ireland.

The primary objective of this work is to propose an approach to analyzing the access-control vulnerabilities that can arise from using Personal Digital Assistants (PDAs) as part of an application system. While PDAs are typically single-user systems supporting little or no access-control, they are expected to synchronize with multi-user host systems that do have access-control requirements. This synchronization may be used to bypass host system access-controls.

For example, an employee working in sales and engineering departments is subject to the security requirement that sales data may not be written to engineering datasets. If we are not confident about the employee's PDA upholding this requirement then synchronization must ensure that at any one time, either sales or engineering information is carried on the employee's PDA, but not both. Other scenarios are possible, for example, the PDA carries both engineering and sales datasets for information purposes. However, only sales data can be two-way synchronized with the host system.

Achieving this security analysis requires a paradigm-shift on what an access-control policy represents. Conventional access-control policies specify the access constraints that are to be enforced by a protection mechanism such as a security kernel or security-wrapper based architecture. We depart from this view by assuming that an access-control policy defines the access-limitations that we believe to be reflected by a particular component; whether upheld explicitly by a protection mechanism or implicitly as a result of our belief in the way a component with no protection mechanism behaves. Thus, while a PDA such as a Palm handheld does not have an access-control mechanism, we can still specify, albeit with low confidence, the access limitations that we believe the installed software implicitly provides.

Our approach leads to a new paradigm for modeling and analyzing the access-control vulnerabilities of systems that are comprised of components of varying security. These components represent systems, handhelds, or alternatively, COTS components whose potential accesses are articulated as a security policy. It is not necessary for these components to have an *explicit* access control mechanism; the security policy represents the access limitations that we believe the component effectively upholds. Thus, in one sense, every component in the system can be regarded as contributing (in varying degrees) to the overall trusted computing base. In our framework we can distinguish the merit of each component's contribution. Security analysis determines how the interaction between these statements influences our confidence in security being upheld.