Дополнительные механизмы безопасности в операционнной системе Linux

А.В. Галатенко <agalat@msu.ru>, А.А. Наумов <aln@msu.ru>,
А.А. Жеглов <ashcan@castle.nmd.msu.ru>

Как только речь идет о предоставлении какого-то сервиса в сети Интернет, необходимо задуматься об обеспечении информационной безопасности данного сервиса, то есть о выполнении политики безопасности, которая предусмотрена разработчиками и владельцем сервиса. В Центре телекоммуникации и технологии Интернет МГУ им. М.В.Ломоносова ведутся работы по увеличению безопасности операционной системы Linux, используемой в ядре сети МГУ.

Выбор системы Linux в качестве основной операционной системы продиктован следущими соображениями: свобода распространения, открытость кода, наличие большого числа прикладных программ. Дополнительные механизмы безопасности можно разделить на две части: первая - это изменения в ядре операционной системы, и вторая - модификация и создание новых прикладных програмных продуктов, удовлетворяющих заданым требованиям.

Для успешного функционирования различных сервисов необходимо предоставлять приложению возможность по аутентификации/авторизации пользователей. В системе данный сервис возложен на библиотеку встраиваемых неинтерактивных модулей аутентификации PNIAM (Pluggable Non-Interactive Authentication Modules), разработанную в МГУ. При использовании PNIAM доступ к файлам с информацией о пользователях осуществляет не приложение, как в классической схеме, а модуль, что позволяет внести гибкость в настройки системы, поскольку приложение не обязано знать про структуру файлов с реквезитами пользователей. Для использования совместно с данной библиотекой были модифицированы такие программы как su, login, passwd, chfn. Кроме этого на база анонимного ftp-сервера libra был написан ftp-frontend для использования с PNIAM, также openssh был портирован под данную технологию.

Как правило, на компьютере, предоставляющем какие-либо сервисы в сети работает достаточно большое количество приложений. Поэтому задача изоляции приложений приобретает еще большую важность. Нами эта задача была решена путем внедрения в ядро операционной системы Linux (в качестве базового было взято ядро версии 2.2.14) механизмов мандатного разграничения доступа, в том числе и на уровне сети. Мандатный механизм разграничения доступа был выбран не случайно, поскольку он фигурирует в требованиях к построению операционных систем с большим уровнем защиты. Также был улучшен дискреционный механиз разграничения доступа, путем использования наработок Andreas Gruenbacher. Для работы с новой моделью разграничения доступа часть системных приложений была изменена, а часть была написана заново.

Для успешного контроля работы компьютера необходимо осуществлять протоколирование различных событий, поэтому ядро операционной системы было модифицировано для использования новой схемы протоколирования. Также для этого был модифицирован демон по сбору лог-записей.