XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.172-173

УДК 50.41.00

Р.Н.Трачук (5 курс, каф. ИБКС), М.О.Калинин, ст. преп.

АУТЕНТИФИКАЦИЯ В ОС WINDOWS 2000/XP

Windows 2000/XP производит аутентификацию при входе пользователя в систему. В большинстве случаев этого достаточно, так как система автоматически выполняет разграничение доступа на основании имени пользователя, вошедшего в систему. Более того, Microsoft не рекомендует встраивать собственные механизмы аутентификации в приложения, следуя принципу единого входа (Unified Logon) - пользователь должен ввести имя пользователя и пароль только один раз при входе в систему.

Для аутентификации существует три способа:

- с помощью функции LogonUser;
- с помощью Security Support Provider Interface (SSPI);
- способ, основанный на функции NetUserChangePassword.

Функция LogonUser в Win32 API непосредственно предназначена для решения задачи аутентификации. Использование функции LogonUser совсем несложно, однако у нее есть одно очень существенное ограничение в Windows NT и Windows 2000: вызывающий эту функцию пользователь должен иметь привилегию SE_TCB_NAME. Это очень сильная привилегия, настолько сильная, что даже администраторы не имеют этой привилегии. Фактически, эта привилегия означает полный контроль над системой, TCB в ее названии расшифровываются как Trusted Computing Base - часть компьютерной системы, которая обеспечивает выполнение политики безопасности. TCB включает в себя код, исполняющийся в режиме ядра, а также код пользовательского режима, исполняющийся в контексте учетной записи, имеющей TCB-привилегию.

SSPI – это вариация стандарта Generic Security Service API (GSS-API), реализованная Microsoft. Идея обоих интерфейсов заключается в том, что все протоколы сетевой аутентификации, будь то NTLM, Kerberos или SSL, могут быть представлены в виде упорядоченного обмена сообщениями, в ходе которого одна из сторон аутентифицирует другую (или стороны взаимно аутентифицируют друг друга).

SSPI сам по себе является лишь интерфейсом, предоставляющим стандартизованный доступ к различным пакетам безопасности (security packages). В составе Windows NT 4 поставляется только один пакет безопасности, NTLM, который можно использовать для аутентификации пользователей. Начиная с Windows 2000 в дополнение к пакету NTLM присутствуют пакеты Kerberos и Negotiate. Мы будем использовать NTLM, так как этот пакет доступен во всех версиях Windows NT

Важным преимуществом данного метода перед методом с использованием функции LogonUser является то, что для его использования не требуются никаких привилегий. Недостаток состоит в том, что этот метод всегда реализует сетевой вход в систему (LOGON32_LOGON_NETWORK), что не всегда приемлемо (но если мы хотим всего лишь проверить правильность имени и пароля пользователя, это не имеет значения).

Наконец, можно проверять правильность имени пользователя и пароля с помощью функции NetUserChangePassword, установив при вызове этой функции новый пароль идентичным старому. Применение данной функции довольно легко.

Главная проблема этого метода состоит в том, что функция NetUserChangePassword не предназначена для аутентификации пользователей. Использование ее не по назначению может принести проблемы с той стороны, с которой вы даже не ожидаете.

Проделанная работа.

Разработанный продукт состоит из 4 частей: Locker.exe, Syshook.dll, Sysblock.dll, Intercepter.exe.

Рассмотрим процесс работы продукта: после запуска Locker.exe находит работающий процесс Explorer.exe, создает в нем поток и загружает в поток Syshook.dll. Созданный нами поток загружает Sysblock.dll во все процессы в системе и приостанавливает свою работу до прихода уведомления об окончании работы, после чего выгружает Sysblock.dll из всех процессов в системе. Sysblock.dll блокирует все вызовы на запуск приложений, определенных в appx.ini. После запуска Intercepter.exe происходит аутентификация пользователя, если аутентификация происходит удачно, то отсылается уведомление об окончании работы, и происходит выгрузка Syshook.dll из Explorer.exe.

Такая архитектура “прячет” работу по блокированию в потоке процесса Explorer.exe, в системе не появляется новых процессов, и завершить блокирование с помощью CTRL+ALT+DEL невозможно. Снятие блокирования возможно лишь после аутентификации.