УДК 004.451.642

ОРГАНИЗАЦИЯ ДОПОЛНИТЕЛЬНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ В WINDOWS XP АЛЬТЕРНАТИВНЫМИ СРЕДСТВАМИ

Щербаков А.С., Теплинский С.В.
Донецкий национальный технический университет

Развитие и распространение информационных технологий спровоцировало стремительное развитие новой отрасли – защиты информации. На сегодняшний день защита и шифрование данных для многих фирм и организаций являются критически необходимыми. Многие компании закладывают значительную часть бюджета в организацию безопасности данных. Однако в большинстве случаев требуется найти простое и дешевое решение, которое бы не потребовало значительных инвестиций и привлечения большого числа кадров. Особенно следует отметить локальный взлом, при котором атака взломщика направлена на локальный компьютер и сам взломщик имеет физический доступ к компьютеру (зачастую в подобных ситуациях взломщик сильно ограничен во времени).

В данном случае эффективными могут оказаться нетрадиционные способы защиты, они направлены на затруднение локального взлома и отпугивание лица, пытающегося получить доступ к компьютеру, любыми доступными способами. Рассмотрим простую возможность блокировки несанкционированного доступа, которую использует разработанная для демонстрации программа, а также рассмотрим алгоритм работы программы. Для осуществления такой блокировки необходимо создать приложение, которое непосредственно производит идентификацию пользователя, желательно без использования пароля, а с использованием альтернативных способов. Например, для идентификации пользователя можно использовать flash-накопитель и производить проверку наличия определенного файла на нем или проверять серийный номер накопителя. После успешной аутентификации приложение должно инициализировать загрузку интерфейса пользователя. Наиболее простой способ интегрирования приложения в систему – установить приложение в качестве интерфейса пользователя (оболочки). По умолчанию оболочкой является Explorer.exe. Изменить оболочку для текущего пользователя можно, используя реестр windows, за интерфейс текущего пользователя отвечает параметр «HKEY_CURRENT_USER\Software\Microsoft\Windows\ CurrentVersion\Policies\system\shell» [1] типа REG_SZ. Данный параметр необходимо вносить в реестр при установке программы или при ее конфигурации. Путь можно не указывать, если программа лежит в системной папке. Следует отметить, что правами записи для указанных разделов реестра обладают только пользователи, входящие в группу администраторов, что предотвращает непреднамеренное или преднамеренное изменение соответствующих ключей пользователями.

Однако установка собственной оболочки не запрещает пользователю нажать Ctrl+Alt+Del, тем самым, вызвать диспетчер задач, и запустить любое другое приложение, в том числе и Explorer.exe. Для запрета вызова диспетчера задач необходимо в реестре создать параметр «HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\ Policies\system\ DisableTaskMgr» [1] типа REG_DWORD со значением 1. Программно это можно реализовать следующим образом (приведен код для Delphi)[2]:

```
var
reg:TRegIniFile;
```

```
begin
Reg:=TRegIniFile.Create('MyApp');
try
  reg.RootKey:=HKEY_CURRENT_USER;
  reg.WriteBool('\Software\Microsoft\Windows\CurrentVersion\Policies\System',
'DisableTaskMgr',true);
finally
  Reg.Free;
end;  end;
```

Включить диспетчер задач, если он был отключен таким кодом, можно только удалив созданный параметр (установка в 0 не поможет из-за несоответствия типа созданного ключа), что создает еще один «подводный камень» на пути потенциального взломщика. После успешной альтернативной аутентификации пользователя необходимо разрешить вызов диспетчера задач и загрузить стандартную саму оболочку. Удаление параметра из реестра можно выполнить сделать следующим кодом:

reg.DeleteKey('\Software\Microsoft\Windows\CurrentVersion\Policies\System', 'DisableTaskMgr');

Необходимо отметить, что в системе MS Windows XP оболочка пользователя загружается раньше приложений, указанных в списках автозагрузки, в том числе и антивирусных пакетов (например, компонент проактивной защиты Антивируса Касперского 6.0 и выше), что не позволяет пользователю снять приложение средствами антивирусной системы. В некоторых ситуациях использование стандартного пароля пользователя невозможно в силу различных обстоятельств (например, для запрета сетевого входа в систему достаточно создать учетную запись пользователя без пароля или удалить пароль существующей). В таких случаях описанный способ является одним из немногих доступных для защиты системы, однако надежно обезопасить компьютер можно лишь при комплексном применении стандартных и альтернативных средств. Кроме того, стандартные пароли Windows достаточно ненадежны, ввиду наличия большого количества программного обеспечения, позволяющего узнать пароль пользователя, особенно если пароль не отвечает требованиям сложности, в то время как альтернативная программа аутентификации будет хранить пароли отдельно от стандартных и может применять другие (в том числе и неповторимые) алгоритмы их шифрования и может использовать любые способы аутентификации пользователя с аппаратной привязкой.

Однако рассмотренный метод вместе с большим числом преимуществ имеет ряд недостатков, а именно: 1) необходимо сделать невозможным изменение, удаление, переименование исполняемого файла программы; 2) нет возможность оперативной блокировки компьютера – для блокировки необходимо выполнять выход из системы.

Рассмотренный способ при правильном подходе позволяет легко обеспечить достаточно надежную защиту компьютера от несанкционированного локального доступа, однако, как и все аналогичные средства защиты, является уязвимым перед загрузкой другой операционной системой, что открывает полный доступ к файловой системе.

Литература

[1] J.Honeycutt *Microsoft Windows XP registry guide. Microsoft Press, Microsoft Corporation, Redmond, Washigton, USA, 2003 – 656 p.*

[2] М.Е. Фленов *Программирование в Delphi глазами хакера.* БХВ-Петербург, СПб, 2004 – 368с.