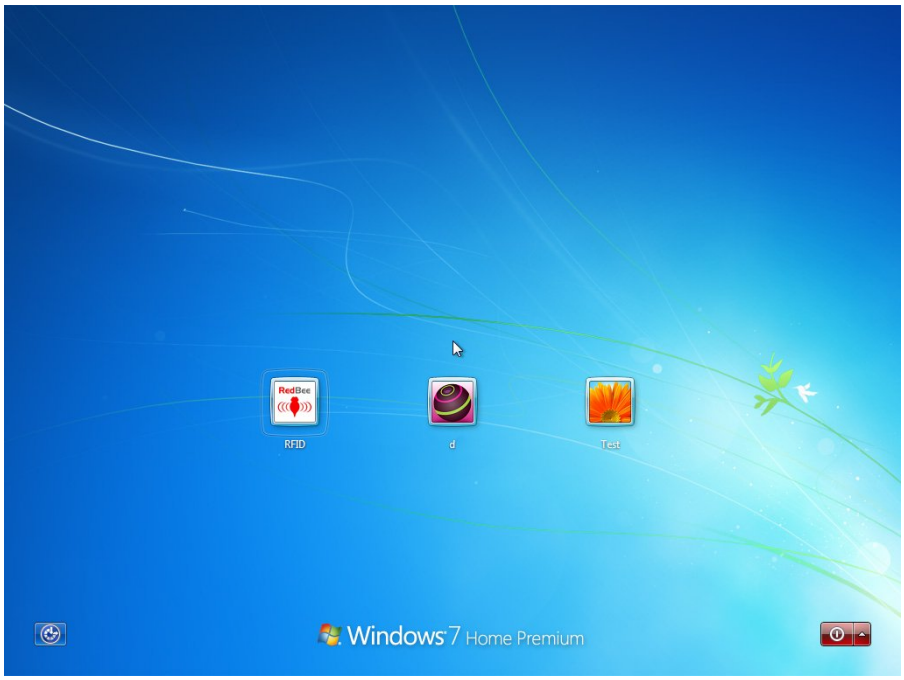
Vista/Win7 RFID Login

By Amal Graafstra, http://www.amal.net/

The RFID Login project for Windows Vista and Windows 7 will enable you to use an RFID tag to log in to Windows. You can assign an RFID tag to any local user account or even corporate domain user accounts, then use that tag to log in rather than typing the account password.

Since the release of Windows Vista, my book readers and forum members have been asking for a Vista/Windows 7 compatible update to the popular Windows XP RFID login project RFIDGina. It wasn't until the release of the new RedBee RFID reader and my own switch from XP Pro to Windows 7 that I decided it was time. The way Windows authenticates account credentials has drastically changed from the old GINA model… and with good reason.

The old GINA model made it very difficult to attach new types of authentication mechanisms to the system, and using more than one new method was nearly impossible. The platform was also not friendly to developers at all. At best, the method of attaching new authentication methods to the GINA was nothing short of a hack. From Vista onward however, Microsoft got rid of the entire GINA mess and approached the authentication system with developers and expandability in mind. They came up with the Windows Credential Provider system, which has clearly documented interfaces and there are even several downloadable code examples. It is this example code I use as a basis for the RFID Login project.



RFID Login

Installation

The RFID Windows Credential Provider has no installation or setup to run. You have to manually make changes to some files and copy them to the right place on your computer to get the precompiled example working.

Unpacking and renaming files

First open the project ZIP file and copy the files from the Release folder to a temporary location on your computer. You should now have the following files on your computer;

Register.reg
RFIDCredentialProvider.dll.32
RFIDCredentialProvider.dll.64
RFIDCredentials.txt
RFIDCredSettings.txt
Unregister.reg

You need to rename the appropriate version of **RFIDCredentialProvider.dll** file for your operating system. If you are using a 32 bit operating system, rename **RFIDCredentialProvider.dll.32** to **RFIDCredentialProvider.dll**, and if you're using a 64 bit system, rename the **RFIDCredentialProvider.dll.64** file.

This project was put together as an example only and should not be considered ready for use in an environment where actual security is required. The files used to store configuration settings and user account credentials are not encrypted in any way. At a bare minimum, additional error handling routines and encryption mechanisms should be integrated to protect sensitive information and ensure reliable operation before it should be used outside of a testing environment.

Edit RFIDCredentials.txt

Now you're going to edit the RFIDCredentials.txt file so it lists your RFID tag IDs and the account information you want to associate with each of those IDs. The format of the file is simple. Each line stores a tag ID/account match-up, separated by the pipe " | " character. The file contains the following examples;

12 21 31 13 104|test|mypassword
104 21 31 13 12|domain\test2|mypassword

The first line matches tag ID ***12 21 31 13 104*** with the local machine user account ***test*** and password ***mypassword***. The second line shows how to match a tag ID to a domain user account. Domain accounts typically apply only to businesses where computers are attached to a corporate network.

Edit the file and change the tag IDs, usernames, and passwords to match your tag IDs and user accounts. Be sure to match tag IDs with valid user accounts on your computer!

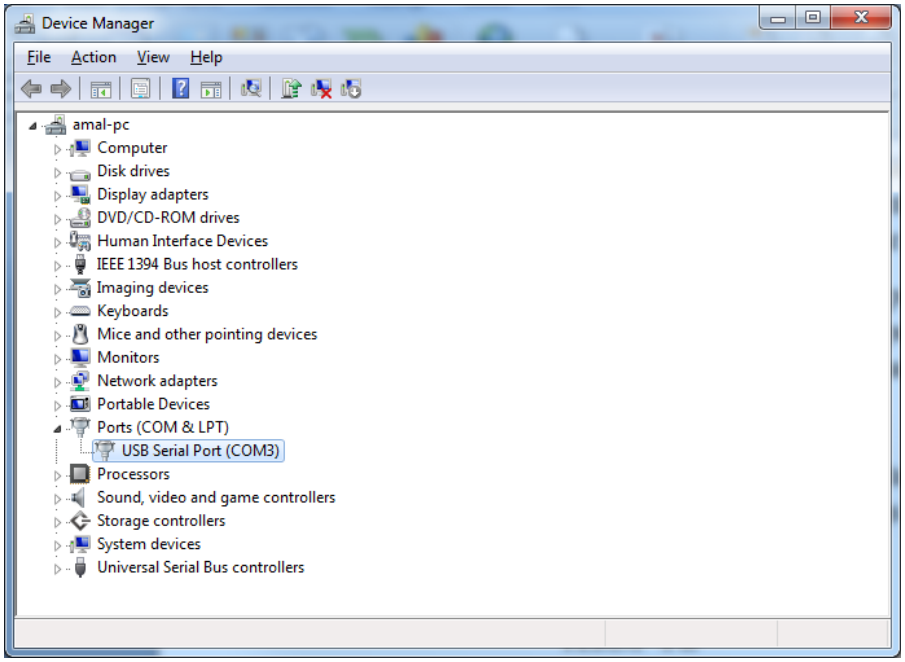
You can list more than one tag ID per account, so more than one RFID tag can log in as the same user name. However you cannot list more than one account per tag ID. If a tag ID is listed more than once in the file, only the first user account to list the tag ID will be logged in.

Edit RFIDCredSettings.txt

The RFIDCredSettings.txt file contains three critical settings used by the credential provider. Here are the default settings that are listed in the settings file;

COM=3
LEAD=ACK
TERM=\r\n

The first line lists the serial COM port that the credential provider will talk to the RFID reader on. If you are using the USB cable to connect the reader to your PC, find out what virtual COM port it has been assigned. To do this, click the Windows button on the task bar and type Device Manager. In the dynamic search results window you should see Device Manager pop up under the Control Panel heading. Press Enter on the keyboard or click the Device Manager listing. Click on Ports to expand the list and you should see an entry called USB Serial Port and in parenthesis it should list the COM port number assigned to it. On my computer that port is COM3, but it could be anything from COM1 to COM255 on yours.



RFID reader USB serial port assigned to COM3

Take note of the COM port number and change the COM= line in RFIDCredSettings.txt to match. The next line has to do with how the RFID credential provider knows when to start matching data from the RFID reader to tag IDs listed in the RFIDCredentials.txt file.

The LEAD setting simply lists the characters the RFID reader will output just before the tag ID starts. The default is actually four characters; The first three are ACK and the last character is a space. That space is very important, and if it is not listed, your tag IDs listed in RFIDCredentials.txt will not match. However, you can omit the space in the LEAD setting if you start your all your tag IDs in RFIDCredentials.txt with a space character.

The default "ACK " setting will catch tags stored in the RFID reader's internal memory as well as tags that aren't stored. It will also catch tag reads from single readers in normal mode and multiple readers with XB mode turned on. If you are using multiple readers that all communicate on the same XBee BPAN and have XB mode turned on, you may consider changing the LEAD setting to match the multi-reader tag ID output format. If the reader at your computer desk has a device ID of 5 and the tags are not stored in the reader's internal memory, then the LEAD setting should look like this;

@5:T:NACK

Don't forget the space character after the K in NACK!

The last setting is called TERM which stands for termination. These characters that signal the RFID reader has sent the full RFID tag ID. The default TERM setting is \r\n which means a CRLF or carriage return character and a line feed character. This setting should really never be changed, but it's nice to have the option so I made it a configurable setting.

Copying files to C:\Windows\System32

Now copy the following files to the C:\Windows\System32 folder;

RFIDCredentialProvider.dll
RFIDCredentials.txt
RFIDCredSettings.txt

If you have installed Windows on a different drive or to a non-standard path, you will have to update the project source code to point to your OS system32 path and recompile the RFIDCredentialProvider.dll file. You will also have to update the Register.reg file to point to the correct system32 path.

Register the new credential provider

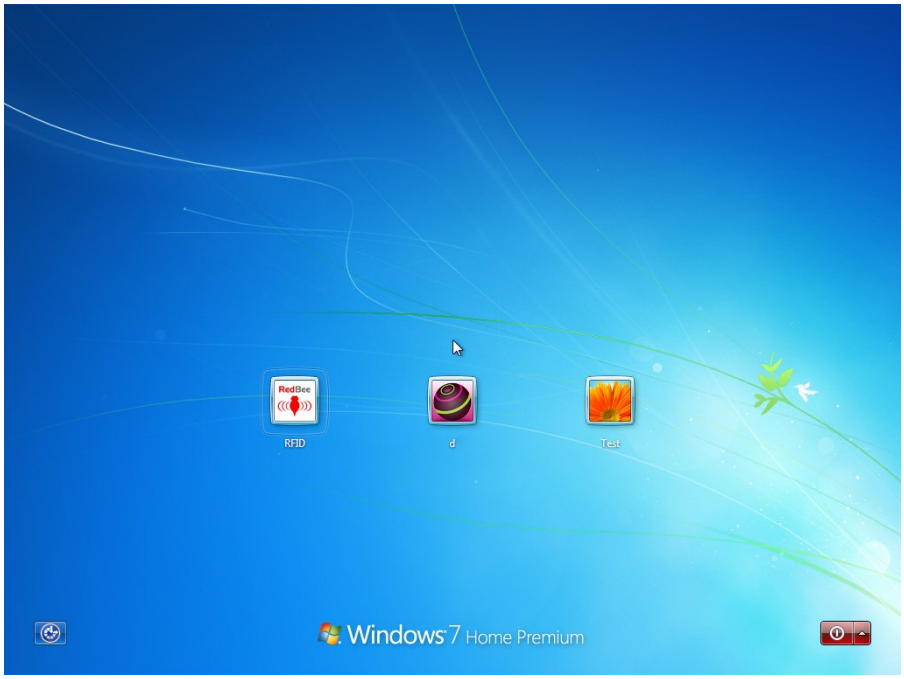
Now double click the Register.reg file and import the associated registry values into your local computer's registry.

Using RFID Login

After registering the new provider using Register.reg, you can use the new provider. You can use RFID login to do the following;

- Initial user login after starting your computer
- Unlocking a locked workstation or user session
- Switching users

When presented with a logon tile screen, you will notice a new tile called RFID amongst your regular user account tiles. The RFID tile has the picture of a RedBee reader logo, which is hard-set in the project source code. *NOTE: You may have to click the “Switch User” button in order to see the logon tile screen.



RFID User Tile

If you want to change the tile image, you will have to modify the project source code. First create a 128x128 size 24 bit BMP image icon and overwrite the tileimage.bmp file in the project source code folder. Then simply recompile the RFIDCredentialProvider.dll file and copy that new file overtop the old one in your Windows\System32 path.

To login, just present a tag to the reader and if the ID is found in the RFIDCredentials.txt file, the associated username and password will be used to log in with!

Securing RFIDCredentials.txt

As noted before, to truly secure the user account data stored in RFIDCredentials.txt you should update the project source code to institute some type of encryption mechanism. However, you can at least remove unnecessary access to the file by updating its NTFS file permissions. Remove every account from the security list except SYSTEM and at least one local administrator account (so you can still update the file later). Of course, if you commonly log into your system using an administrator account, securing the file in this way won’t do much.

Need help?

If you have any questions regarding this project, please post them to the user forum at http://www.rfidtoys.net/forum