SHA-1 Authentication Demo

Hardware

- 1-Wire adapter (DS9097U-S09, DS9097U-E25, or DS9490R)
- One or more DS2432 or DS1961S devices
- 1-Wire Memory Evaluation board with socket for DS2432 or DS1402D-DR8 blue-dot for DS1961S
- RJ11 cord to connect from evaluation board to 1-Wire adapter for DS2432

Installation

1. 1-Wire Drivers

Run file: 'install_1_wire_drivers_v400b4.msi' in the folder 'Drivers'
When prompted select the adapter to use and port to use for the demo.

Web: ftp://ftp.dalsemi.com/pub/auto_id/licensed/install_1_wire_drivers_v400b4.msi

2. OneWireViewer

The 1-Wire drivers will create a folder off the start menu under 'Programs/1-Wire Drivers'. Click on the icon 'OneWireViewer'. This will open the HTML document 'OneWireViewer.htm' in the default browser. This document will describe the installation procedure to run the 'OneWireViewer' application. Typically this involves installing 'Java Web Start' from Sun Microsystems. Connect the 1-Wire adapter and verify 'OneWireViewer' can find the DS2432 connected.

3. Visual Basic 6.0 Runtime:

Run file: 'VBRun60sp5.exe' in the folder 'Drivers'
These drivers are required by the Visual Basic Authentication demo.

Web: http://support.microsoft.com/default.aspx?scid=kb;EN-US;290887

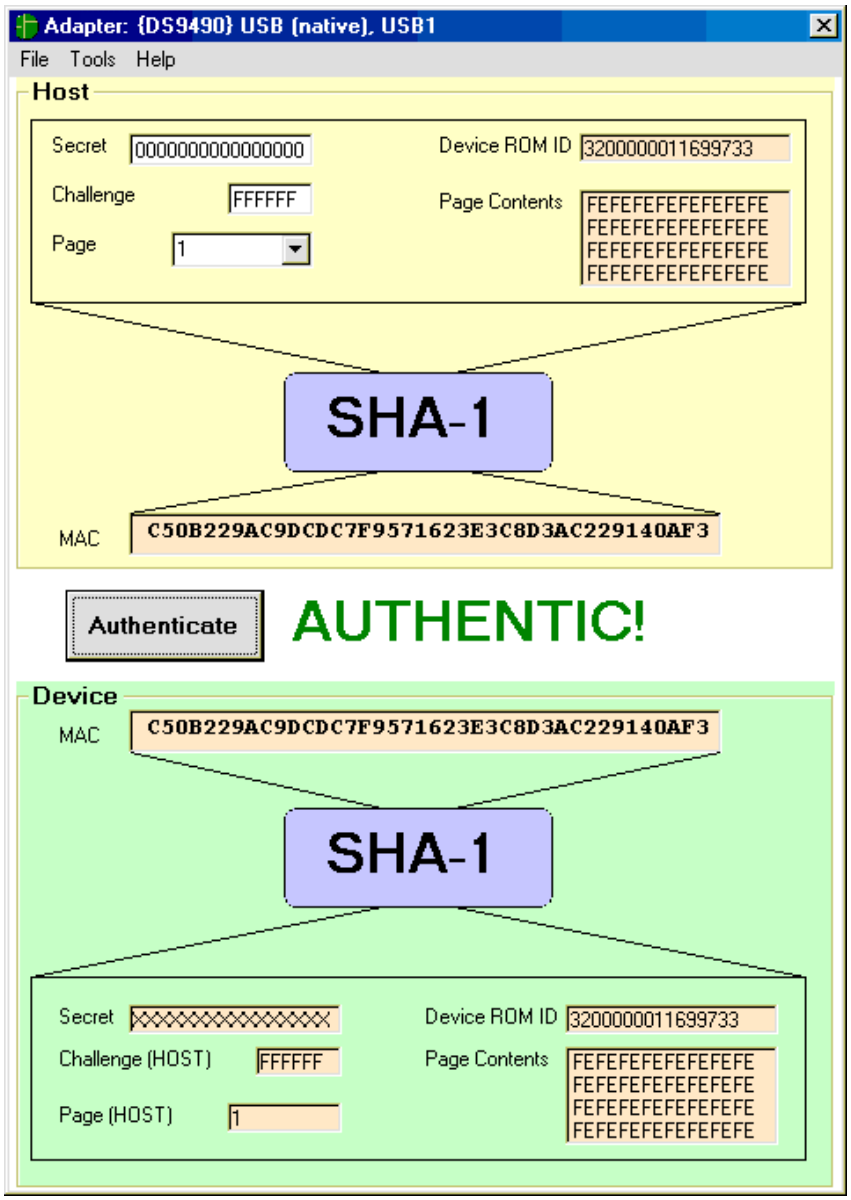
4. Authentication Demo

Copy the file 'Authenticate.exe' to a folder on the PC. Run this application to do the Authentication Demo. This application is written in Visual Basic 6.0. The source is provided in the 'Source' folder.

Authentication Demo

Intro

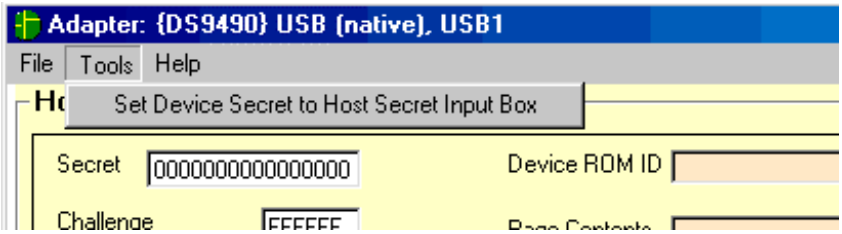
This program visually demonstrates the authentication process that occurs in the 1-Wire device and in the host PC or microcontroller. The Host in the top portion of the demo screen takes the Secret, Challenge, Page number as input by the user and the Device ROM ID and Page contents from the 1-Wire device and uses the SHA-1 algorithm to create a MAC. The same challenge is provided to the 1-Wire device (lower green section) and it's own SHA-1 calculation. If the device and the host come up with the same MAC then the device is authentic and its memory contents are valid. If the MAC is not the same then the device has a different secret and is not authentic. The Challenge is used to make sure each transaction is unique. Writing different data to the Page Contents during the authentication can further enhance this.



There are three inputs in white that the user must select. The Secret is 16 hex characters. The Challenge is 6 hex characters. The page select is a drop-down box where the page number 1-4 can be selected.

Device Setup (Authentication Demo)

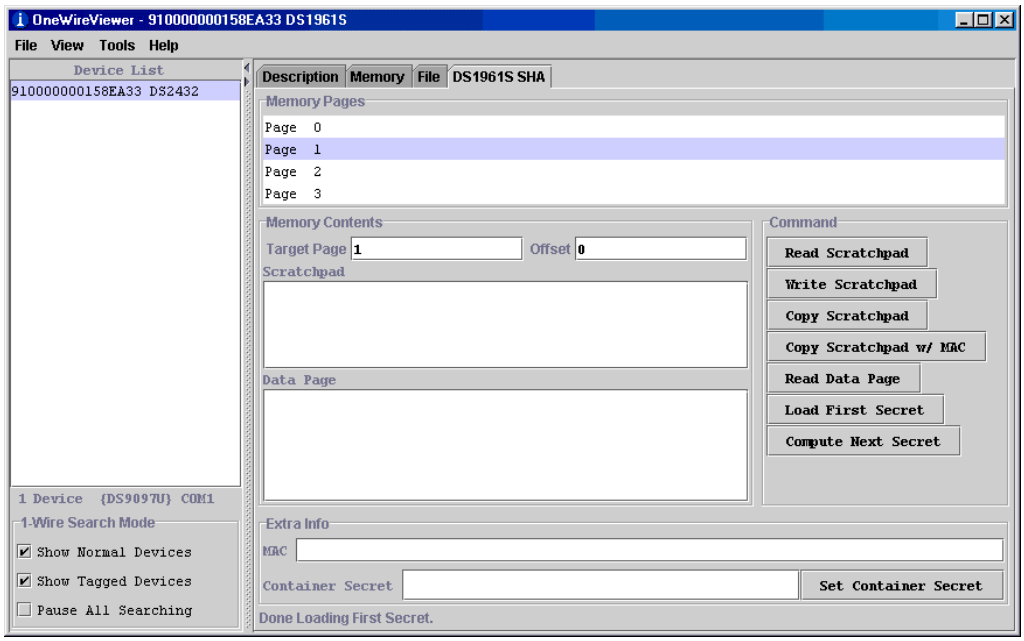
One or more DS2432/DS1961S devices must be initialized with know secrets before using the Authentication demo. The Authentication demo has a menu option for taking the secret entered in the Host Secret Input Box and using that to set the device secret. See menu option below. Note that the secret must not be write-protected. The Authentication demo has no facilities to set user memory at this time, see the Device Setup (OneWireViewer) to set user memory.



Device Setup (OneWireViewer)

One or more DS2432/DS1961S devices must be initialized with know secrets before using the Authentication demo. Run the 'OneWireViewer' that was setup during the installation procedure.

1. Connect the first DS2432 to the 1-Wire network with 1-Wire memory evaluation board. The DS2432 device should show up in the Device List on the left hand side of the windows. If the Device List displays 'DS1961S' then click on the menu 'View/Show Device Alternate Names'.
2. Select the device by clicking on it. Several tabs will now appear in the right side of the windows
3. Click on the 'DS1961S SHA' tab. Note that the DS1961S is the DS2432 in an iButton package.
4. Click the 'Load First Secret' button
5. Type in the secret for the device. (Suggest all 0's for at least one of the devices)
6. Click on the 'Memory' tab
7. Click on a section of memory to read. The sections are: Page Zero, Page One, Page Two and Three. Note that the memory sections are grouped based on memory options.
8. The memory contents will be displayed in the lower right in HEX. The hex data can be edited and changed on the device by clicking 'Commit Changes'.
9. Repeat for other DS2432/DS1961S devices



Demo Scenario

The following provides a suggested demonstration scenario to highlight the authentication features of the DS2432. Start the Authentication demo. It will automatically select the default 1-Wire port selected during 1-Wire driver installation. If a new port needs to be selected then run the 'Default 1-Wire Net' icon in the '1-Wire Drivers' folder under the start/programs menu. It the adapter is not detected then a message will appear after several seconds of attempting to open the port.

Lesson 1 - Show Authentic device

1. Set secret
2. Set challenge
3. Leave default page 1
4. Click the 'Authenticate' button
5. See MAC's generated by the Host and the Device and note that they match

Lesson 2 – Show New Challenge

1. Change challenge to a new value, could be as little as 1 bit different
2. Click the 'Authenticate' button
3. See MAC's generated by the Host and the Device and note that they match. The message 'AUTHENTIC' is displayed in green. Also note that they are completely different then the previous MAC even though the challenge only changed slightly.

Lesson 3 – Show Not Authentic

1. Change secret to a new value, could be as little as 1 bit different
2. Click the 'Authenticate' button
3. See MAC's generated by the Host and the Device and note that they do not match. The message 'NOT AUTHENTIC' is displayed in red. Note how completed different the output is even though the secret only changed slightly.

Lesson 4 – Show New Device with Different Secret

1. Set secret to match new device
2. Connect a new device
3. Click the 'Authenticate' button
4. See MAC's generated by the Host and the Device and note that they match. The message 'AUTHENTIC' is displayed in green. Also note that they are completely different then the previous MAC even though the challenge only changed slightly.
5. Drive home point that we recommend a unique secret for each device. There is a built-in feature that can generate a unique secret by using the SHA engine and the ROM ID.