ALLservice

Password recovery procedure for IBM ThinkPads
using R24RF08 and IBMpass

1. Introduction.

As you probably knew, IBM ThinkPad uses a small eeprom (ATMEL 24RF08) to store different OEM issues like serial number, UUID, etc. The supervisor password (SVP) is stored also into this little chip. So, anybody should figure that he needs to read the eeprom in order to find the password string. The first problem is that 24RF08 is not an ordinary eeprom. The second is that the password is written in a special scan code.
To read this properly you need a software (and an interface) specially designed for this eeprom.
This software is R24RF08 (eeprom reader) and IBMpass (password revealer).

2. Locating the eeprom. Soldering.

You don't need to unsolder the 24RF08 eeprom, just solder 3 wires to SDA, SCL and GND pins of the eeprom. There are two eeprom layouts (see interface schematics described bellow), corresponding to 8 pin or 14 pin eeproms. Locate the eeprom first according to your model (E.g. T20-23 and T30 have the eeprom underneath TP, and can be accessed by removing the RAM modules cover, no need to dismantle the laptop.) and solder the wires using a soldering iron with a fine tip. Also, you can use 0.15 -0.20 mm enamel coated wires or similar small diameter insulated wires. These wires will be connected later to the interface.

As a tip: You can use clips to connect the wires or you can solder on the PCB traces leading to the eeprom pins. Once again, be careful and double, triple check the soldering if necessary till you are positively sure you have done the right job.

3. Choose and build the interface.

Since version 2.0, R24RF08 and W24RF08 are compatible with a wide range of eeprom programmers. By default, both programs set the COM port signals to use direct logic level to access I2C bus. We provide here 2 schematics that are relevant for direct logic signals and for inverse logic signals (**simple-i2cprog.pdf** and **driven-i2cprog.pdf**). Also, depending of the interface you build, you can invert the logics for SDA-In, SDA-Out, and SCL COM port signals by some command line parameters described later in this document.

a) The file **simple-i2cprog.pdf** contains the schematic diagram of a simple interface (known as SI-PROG) based on 2 zeners and 2 resistors. This is a classic, easy to build circuit and works with soldered or unsoldered eeproms. The purpose of the 2 zeners is to convert RS232 levels (+/- 5V) to TTL ones, needed by the eeprom. It uses direct logic signals to I2C eeprom and is powered by the COM port. However, this interface works with in-system eeproms but is dependant on COM port current and eeprom bus impedance. R24RF08 works natively with this circuit, no need to change the lines signals with command line parameters. This circuit works pretty well with almost all Thinkpads series.

b) The second interface is described in **driven-i2cprog.pdf.** The circuit uses MAX 232 as a RS232 to TTL driver and its main purpose is to work with soldered eeproms. The advantage of MAX232 is the TTL outputs that are more reliable and more powerful when work with soldered, in-system eeproms (dependency free from the COM port current). Due of the internal inverters of MAX232 the interface responds to an inverse signal logic level. R24RF08 needs /x, /d, /i switches to be specified in the command line.

What these switches mean:
/x - invert serial clock, also known as SCL;
/d - invert serial data output, also known as SDA-Out;
/i - invert serial data input, also known as SDA-In.

All those can be used in any combination to meet the interface specification.

4. How is it working:
Prepare your technician PC by connecting the interface to the COM1 port (don't connect the wires to eeprom yet). Turn on the ThinkPad and press F1 to enter BIOS Setup. When you are prompted for the password and there's no other activity like HDD access or so, connect the wires (GND first!, SDA, SCL) to the corresponding wires from the interface (attached before to COM1) and execute R24RF08:

-for SI-PROG interface (as described in 3.a above):
r24rf08.exe <filename.ext>. where filename.ext is the file where eeprom content will be stored.
Example: **r24rf08 mytp.bin**

-for MAX232 driven I2C interface (as described in 3.b above):
r24rf08.exe <filename.ext> /x /d /i. where /x /d /i are command line parameters (switches) for this kind of interface.
Example: **r24rf08 mytp2.bin /x/d /i**

Use exactly the instructed switches to avoid possible damages to your eeprom data!

The file should be created in the same folder. Finally, disconnect the wires (GND last!) and turn off the ThinkPad by pressing on/off switch.

5. Reveal the password.
Now, you have the .bin file but you need to dump in scan code to retrieve the password. IBMpass 2.0 Lite is a free tool that i wrote specially for this job. Just open the eeprom dump you've created before and search for 0x330, 0x340 lines. The password is located on 0x338 (and 0x340 depending on model) in scan code. For 24C01 eeproms the password is located at 0x38, 0x40. If the password won't work for the very first time then your eeprom may use newer IBM encryptions. In this case switch to alternate scan codes to find it. For those who want quick answers the recommended version is IBMpass 1.1. Usage for IBMpass 1.1 (command line only):

ibmpass mytp.bin – use "/a" switch to see in alternate scan code if needed:
ibmpass mytp.bin /a

For some old models like 570 or 770Z you need to execute the eeprom patcher first. This will reset the read protection on the password offset. To do that just execute **patcher.exe** before the reading operation, without rebooting the laptop:

-for SI-PROG:
patcher.exe , then immediately
r24rf08.exe <filename.ext>

-for Driven-I2C (Max232) you must insert the switches:
patcher.exe /x /d /i, then immediately
r24rf08.exe <filename.ext> /x /d /i

W24RF08, the writer version, has included the complete APP reset operation you don't need to use patcher.

Remember, use 3 wires from the interface and 3 wires from eeprom! Connect them after your ThinkPad is powered and disconnect them right after you read the content, before you switch off the laptop.

For other infos regarding R24RF08, W24RF08 and IBMpass you can visit www.allservice.ro.
You can also support those free programs by sending me any eeprom dumps.

Victor Voinea,
Author
allservice@home.ro