ROBOTICS TXT Controller Security Information

The root and ROBOPro accounts

The TXT controller is equiped with an embedded Linux system. The root account allows full access to the Linux system. Root access allows arbitrary system configuration and extension, but also allows to destroy the system with single command. The interface application for ROBOPro does not run under the root account, but under the ROBOPro account. This is a normal limited user account without administrative rights.

The ROBOPro account is sufficient for most applications, including running C / C++ applications. The ROBOPro account has direct access to the graphics frame buffer /dev/fb0 as well as to the touch and keyboard input devices /dev/input/event0 and event1.

For this reason it is recommended to use the ROBOPro account unless there is a good reason to switch to the root account. The password for the ROBOPro account is ROBOPro.

The root password

Introduction

Each TXT comes with a unique 12 character root password, which is set randomly during production. Since ROBOPro requires root access in order to run updates automatically, the password is stored encrypted on the TXT. ROBOPro fetches the encrypted password and decrypts it. Obviously by reverse engineering of the ROBOPro executable or the encryption application used on the device, it would be possible to analyze the encryption mechanism and encyption key, so that this method is not entirely safe. By reverse engineering it would be possible to gain root access to any TXT controller. Of cause this would also require network access to the TXT controller, which is possible via Wi-Fi, USB and Bluetooth. Wi-Fi uses a 12 character random access key, which is reasonably safe. Bluetooth uses a 6 digit random paring key, which is not really safe, so it is recommended to switch off Bluetooth unless you need it. USB requires physical access to the TXT Controller and is considered safe.

It should be noted that the reliability of computer systems usually relies on humans remembering strong passwords. There is no safe way to store passwords such that they can be retrieved automatically. The only solution would be a secure smart chip card and a chip card terminal. Since the TXT controller is intended for children, it is not feasible to request that each user sets and remembers a strong password and enters this password for a software update of the TXT. For this reason we chose the method outlined above - use a random password and store the encrypted password on the TXT, so that it can be retrieved by ROBOPro.

If you believe that the 6 digit Bluetooth key or the 12 character Wi-Fi key plus the hiding of the root password encryption keys in the ROBOPro executable does not give sufficient security, you should set your own root password, as described below. This doesn't have any disadvantages except that updates must be performed manually then.

You can also change the password for the ROBOPro account. ROBOPro does not login using the account except for updates. During normal operation ROBOPro uses network ports (65000 and 65001). Please note that by design the network protocol used by ROBOPro allows arbitrary code execution. ROBOPro compiles programs into binary code like a C compiler, so it does not give much of a security advantage to set the ROBOPro account password. The ROBOPro account has restricted rights, so that there should arise no security issues by this.

Retrieving the root password

We want to give our customers full access to the capabilities of the TXT, so there is a way to retrieve the root password. The root password can be made visible on the settings/info display. In order to avoid problems in schools, this feature is disabled by default. In order to enable displaying of the root password, login as ROBOPro (password ROBOPro) via ssh. The IP numbers used by the TXT are 192.168.7.2 for USB, 192.168.8.2 for WLAN and 192.168.9.2 for Bluetooth connection. As windows ssh client putty is recommended, which can be downloaded for free at:

`http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html`

After ssh login as ROBOPro, execute the following command:

```
echo "showroot=1" > .TxtAccess.ini
```

After a reboot, the root password is shown in menue settings/info.

Disabling root password retrieval

In order to disable the root password retrieval feature, first enable it as described above, them login via ssh as root and execute the commands

```
cd /opt/knobloch
rm .TxtAccess.ini
echo "showroot=0" > .TxtAccess.ini
```

Check with ls -al that owner and access rights of .TxtAccess.ini are such that it cannot be changed by any user except root.

If you disable display of the root password, it is recommended to set your own root password.

Setting your own root password

For ultimate security, please set your own root password. This is done by logging in as root and using the usual passwd command. In addition you should modify the access rights of /etc/init.d/rootpwd.done such that it can be modified or deleted only by root. This can be done by logging in as root and issuing the commands:

```
cd /etc/init.d
chown root:root rootpwd.done
chmod 0700 rootpwd.done
```

If this file is deleted, the TXT creates a new encrypted root password on the next reboot.

Installing updates after setting your own root password

If you change the root password, ROBOPro won't be able to install updates any more. There are two solutions to this. Either you can recreate an encrypted random root password. This is done by deleting the /etc/init.d/rootpwd.done file and rebooting. Alternatively you can copy and run the update scripts manually as root. For this copy the proper update.sh file from the ROBOPro installation folder into the /opt/knobloch folder and execute it as root.