KRACK and BlueBorne vulnerabilities and Digi Embedded Yocto

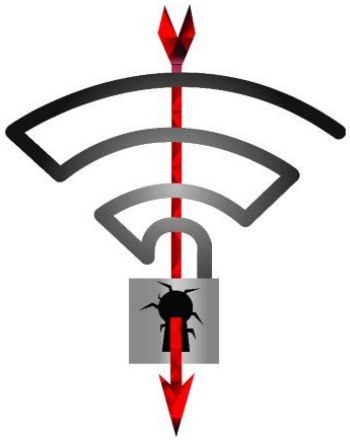
November 2017

Introduction

This document provides instructions for updating Digi Embedded Yocto to integrate fixes for two recently discovered critical vulnerabilities: KRACK and Blueborne.

KRACK

On October 16th, 2017, a public vulnerability was released that impacts the Wi-Fi "over the air" encryption protocol known as WPA/WPA2. The attack is called "KRACK" for "Key Reinstallation Attacks". These vulnerabilities allow an attacker to intercept and in some special cases inject network traffic between a Wi-Fi Client and a Wi-Fi Access Point. This attack can only be performed if the attacker is within radio intercept distance of a Client and Access Point. It is noted that with the discovered vulnerabilities, BOTH the Client and the Access Point must be fixed to fully protect the network traffic. The impact of this vulnerability is only against the transport layer. Other encryption, such as TLS 1.2 that is done at other layers, is NOT impacted and can be considered safe. However, with a corrupted transport layer, it may be possible to conduct other attacks like man in the middle (MitM) attacks by tricking end users.



Digi Wi-Fi products using Digi Embedded Yocto **are affected** by the KRACK vulnerability **when using Client Modes**. Note that **Access Point Modes are not affected** with the default wpa_supplicant/hostap configuration provided with DEY because Fast Transition is disabled.

BlueBorne

The BlueBorne vulnerability affects devices using Bluetooth and allows attackers to take control of devices, access corporate data and networks, penetrate secure “air-gapped” networks, and spread malware laterally to adjacent devices. BlueBorne affects ordinary computers, mobile phones, embedded devices, and other connected devices with Bluetooth connectivity. See https://www.armis.com/blueborne/ for detailed information about the vulnerability. **For embedded SoMs using DEY, Digi strongly recommends that customers integrate the fixes provided through the git repositories.**

Installation instructions

The following step-by-step instructions describe how to incorporate KRACK and Blueborne fixes for different versions of Digi Embedded Yocto.

Go to the Digi Embedded Yocto **layer** folder (the one that contains the **sources** subfolder, not the Yocto workspace) and issue the following commands:

- For Digi Embedded Yocto 2.2:

```
$ repo init -u https://github.com/digi-embedded/dey-manifest.git -b morty
$ repo sync -j4 --no-repo-verify
```

- For Digi Embedded Yocto 2.0:

```
$ repo init -u https://github.com/digi-embedded/dey-manifest.git -b jethro
$ repo sync -j4 --no-repo-verify
```

- For Digi Embedded Yocto 1.6:

```
$ repo init -u https://github.com/digi-embedded/dey-manifest.git -b daisy
$ repo sync -j4 --no-repo-verify
```

This updates the repositories to the latest changes, including the KRACK fixes.

Then go to your Yocto workspace and rebuild the image as usual:

```
$ bitbake dey-image-qt
$ bitbake core-image-base
```

Additional information

Visit Digi Security Center for the latest news about security on Digi's products or contact tech.support@digi.com if you have further questions.

References

1. KRACK vulnerability
2. Blueborne vulnerability