Author: Troy Shurtleff

Building the Vulnerable signApp

This document and the associated source code is intended for course instructors only. Having access to the signApp source code would trivialize part of the reverse engineering exercise.

This document is accompanied by the following files:

```
├── vuln_code
    ├── signApp ← ELF file for the ARM target
    └── signApp.c ← Source code for the signApp
```

The vulnerable signApp can be built on the Reverse Engineering VM provided with this exercise. Note that the delivered Reverse Engineering VM does not contain the signApp source code.

First, copy the `vuln_code` folder to the student users home directory on the Reverse Engineering VM. Using the VirtualBox File Manager is probably the easiest way to do the transfer.

To build the signApp run the following command.

```
student@revm:~$ ~/buildroot-2019.02.4/output/host/usr/bin/arm-buildroot-linux-
uclibcgnueabi-gcc -fno-stack-protector ~/vuln_code/signApp.c -o
~/vuln_code/signApp
```

The command uses the compiler provided by Buildroot for the target hardware.

To include the signApp ELF file in a build of the Variable Message Sign system place it in the `/home/student/buildroot-2019.02.4/overlay/usr/sbin` folder before building the VMS

Instructions for building the VMS are included in the "Building the Variable Message Sign System" document.

Author: Troy Shurtleff
Copyright 2019 BAE Systems
SPDX-License-Identifier: Apache-2.0

Approved for public release; unlimited distribution
Not export controlled per ES-FL-091619-0203