



CV186AH SDK 网络安全二次开发使用手册

Version: 1.0.0

Release date: 2023/12

©2022 北京晶视智能科技有限公司
本文件所含信息归北京晶视智能科技有限公司所有。
未经授权，严禁全部或部分复制或披露该等信息。

目录

1	声明	2
2	概述	3
3	SDK 二次开发网络安全注意事项	4
3.1	u-boot 使用注意事项	4
3.1.1	串口	4
3.1.2	u-boot 指令	4
3.2	Linux 使用网络安全注意事项	5
3.2.1	root 帐户	5
3.2.2	文件权限	6
3.3	Linux 驱动使用网络安全注意事项	6
3.3.1	串口	6
3.4	应用开发安全注意事项	6
3.4.1	Cipher 驱动	6
3.5	其他安全注意事项	7
3.5.1	裸片烧写	7
3.5.2	SD 卡/U 盘挂载权限	7
3.5.3	JTAG	7
3.6	Alios 开发使用注意事项	7

修订记录

Revision	Date	Description
1.0.0	2023/11/10	初稿

1 声明



法律声明

本数据手册包含北京晶视智能科技有限公司（下称“晶视智能”）的保密信息。未经授权，禁止使用或披露本数据手册中包含的信息。如您未经授权披露全部或部分保密信息，导致晶视智能遭受任何损失或损害，您应对因之产生的损失/损害承担责任。

本文件内信息如有更改，恕不另行通知。晶视智能不对使用或依赖本文件所含信息承担任何责任。本数据手册和本文件所含的所有信息均按“原样”提供，无任何明示、暗示、法定或其他形式的保证。晶视智能特别声明未做任何适销性、非侵权性和特定用途适用性的默示保证，亦对本数据手册所使用、包含或提供的任何第三方的软件不提供任何保证；用户同意仅向该第三方寻求与此相关的任何保证索赔。此外，晶视智能亦不对任何其根据用户规格或符合特定标准或公开讨论而制作的可交付成果承担责任。

联系我们

地址 北京市海淀区丰豪东路 9 号院中关村集成电路设计园（ICPARK）1 号楼

深圳市宝安区福海街道展城社区会展湾云岸广场 T10 栋

电话 +86-10-57590723 +86-10-57590724

邮编 100094（北京）518100（深圳）

官方网站 <https://www.sophgo.com/>

技术论坛 <https://developer.sophgo.com/forum/index.html>

2 概述

在基于 CVITEK 处理器解决方案开发的产品有可能面对相关的网络安全威胁，本文主要的目的在于从网络安全的角度针对这些问题提供相应的解决方案。

3 SDK 二次开发网络安全注意事项

3.1 u-boot 使用注意事项

3.1.1 串口

SDK 中的 u-boot 串口功能默认是开启的。在 u-boot 的执行流程中，u-boot 会等待一秒的时间让研发人员可以在执行阶段透过敲击按键的方式中断 u-boot 执行过程以停留在 u-boot 阶段进行调试。若过程中没有任何敲击按键的事件发生，一秒后则会继续 u-boot 的开机流程。

在正式发布的产品，可以将此配置取消，以达到无法在 u-boot 阶段透过串口调试的目的，具体实现方法如下：

步骤 1. 开启 build/boards/{chip_name}/{board_name}/u-boot/{board_name}_defconfig (依据各产品的命名可能会有不同的文件名称，此示例中为 athena2_wevb_0010a_emmc_defconfig)。修改 CONFIG_BOOTDELAY 的配置值为“-2”。

```
CONFIG_IDENT_STRING=" cvitek_athena2"
CONFIG_ARMV8_SET_SMPEN=y
CONFIG_TARGET_CVITEK_ATHENA2=y
CONFIG_DISTRO_DEFAULTS=y
CONFIG_FIT=y
CONFIG_BOARD_LATE_INIT=y
# CONFIG_ARCH_FIXUP_FDT_MEMORY is not set
CONFIG_BOOTDELAY=-2
```

步骤 2. 重新编译 u-boot

3.1.2 u-boot 指令

u-boot 下提供许多研发人员进行开发与调试的指令，例如：md, mw, setenv, saveenv 等。但这些指令在正式产品中并非是必须的。可以选择保留无关乎系统安全的指令，并将其他指令删除。

例如欲删除 md/mw 指令，具体实现方式如下：

开启/u-boot-2021.10/cmd/Makefile, 因为 md/mw 具体实现代码是在 mem.c 中

所以直接将下面示例中的 obj-\$(CONFIG_CMD_MEMORY) += mem.o 注释掉或删除

```
obj-$(CONFIG_LOGBUFFER) += log.o
obj-$(CONFIG_ID_EEPROM) += mac.o
obj-$(CONFIG_CMD_MD5SUM) += md5sum.o
obj-$(CONFIG_CMD_MEMORY) += mem.o
obj-$(CONFIG_CMD_IO) += io.o
obj-$(CONFIG_CMD_MFSL) += mfsl.o
```

或是修改 /u-boot-2021.10/cmd/Kconfig, 将 default 配置为” n”。

```
config CMD_MEMORY
bool "md, mm, nm, mw, cp, cmp, base, loop, ip_update"
default n
help
Memory commands.
md - memory display
mm - memory modify (auto-incrementing address)
nm - memory modify (constant address)
mw - memory write (fill)
cp - memory copy
cmp - memory compare
base - print or set address offset
loop - initialize loop on address range
ip_update - sync ip from mem 0x400038C/900 to uboot env
```

其他命令删除方法与上面的操作类似。

3.2 Linux 使用网络安全注意事项

3.2.1 root 帐户

在实际产品中, 需要对 root 用户做安全性修改, 用户可决定更改默认密码或是禁止 root 透过 shell 登录。具体方法如下:

- 修改密码

步骤 1. 执行 shell 指令” passwd” 更改密码。

步骤 2. 将/etc/shadow 拷贝出来 (可透过挂载 SD 卡或是网络)

步骤 3. 将 shadow 文件拷贝至/ramdisk/rootfs/overlay/{chip_name}/etc 下。

步骤 4. 重新编译 rootfs 文件系统 (指令: pack_rootfs), 并将 rootfs.emmc 重新烧入进平台。

- 禁止 root 透过 shell 登录

步骤 1. 修改 SDK 包里的/ramdisk/rootfs/overlay/{chip_name}/etc/passwd, 将内容

```
root:x:0:0:root:/root:/bin/sh
```

修改成:

```
root:x:0:0:root:/root:/bin/false
```

步骤 2. 重新编译 rootfs 文件系统 (指令: `pack_rootfs`), 并将 `rootfs.emmc` 重新烧入进平台。

3.2.2 文件权限

SDK 默认使用 SquashFS 文件系统, 用户无法对预载的文件系统进行写或删除的动作, 藉此来保护系统的稳定性。

3.3 Linux 驱动使用网络安全注意事项

3.3.1 串口

研发人员在 linux 中可透过串口来做调试, 若要避免串口被非法接入的风险, 确定串口在产品中不再使用, 则在出厂时可以关闭串口。具体实现方法如下:

步骤 1. 开启 `build/boards/default/dts/{board_name}/{chip_name}_base.dtsi` (依据各产品的命名可能会有不同的文件名称, 此示例中为 `cv186x`), 修改如下示例的代码,

```
uart0: serial@29180000 {
    compatible = "snps,dw-apb-uart";
    reg = <0x0 0x29180000 0x0 0x1000>;
    clock-frequency = <200000000>;
    reg-shift = <2>;
    reg-io-width = <4>;
-   status = "okay";
+   status = "disabled";
};
```

步骤 2. 重新编译 linux

3.4 应用开发安全注意事项

3.4.1 Cipher 驱动

CIPHER 是晶视智能数字媒体处理平台提供的安全算法模块, 提供对称式加解密算法包括 AES/DES/SM4, 不对称加解密算法 RSA 随机数生成, 以及摘要算法包括 HASH, HMAC, 客户可用于对音视频码流进行加解密保护, 认证用户合法性等场景。详情请参考《CVITEK CIPHER API 参考》。

3.5 其他安全注意事项

3.5.1 裸片烧写

SDK 包提供 SD，USB 裸片烧写功能，建议在实际产品中将裸片烧写功能关闭。SD，USB 裸烧功能可以透过硬件上的设计进行关闭。

3.5.2 SD 卡/U 盘挂载权限

若开发的产品具备 SD card 或是 U 盘等可插拔储存设备接口时，建议挂载储存设备文件系统前加上” -o noexec” 参数，以避免恶意第三方程序的运行进而造成系统的损坏。

3.5.3 JTAG

建议在实际产品上移除 JTAG 接口，以避免恶意窜改系统配置而造成系统损坏。

3.6 Alios 开发使用注意事项

参考 Alios 开源文档 <https://github.com/alibaba/AliOS-Things/tree/master/documentation>