Compile Argon2 for Android

2018-08-03 | Riguz

Tags: Android, 移动端, 闲话编程

Keepass中使用了一个Argon2的算法来存储用户主密码，这个算法被认为是下一代的较为安全的密码散列算法。

我们来看看 Argon2 算法：

```
hfli@CNhfli ~/Documents/phc-winner-argon2 (master*) $ echo -n "password" | ./argon2 s
Type:       Argon2i
Iterations: 2
Memory:     65536 KiB
Parallelism:    4
Hash:       2748e90a5a301dbcf46067a8784d3e73c7acc8939b4ee02d
Encoded:    $argon2i$v=19$m=65536,t=2,p=4$c29tZWhlbGxvd29ybGQ$J0jpClowHbz0YGeoeE0+c8e
0.126 seconds
Verification ok
```

这个算法又分为两个版本,Argon2i 和 Argon2d:

> Argon2d provides the highest resistance against GPU cracking attacks. Argon2i is designed to resist side-channel attacks.

Keepass 中选择的是 Argon2d

> Only the Argon2d variant of Argon2 is supported (a strong defense against GPU/ASIC cracking attacks is the most important goal, and Argon2d here is better than Argon2i; side-channel timing attacks are basically irrelevant, because KeePass is a local application, not a remote server)

在安卓上编译可以参考如下步骤:

Application.mk

```
APP_BUILD_SCRIPT := Android.mk
APP_STL := gnustl_shared
APP_ABI := armeabi-v7a
```

Android.mk

```
LOCAL_PATH := $(call my-dir)

include $(CLEAR_VARS)

LOCAL_MODULE := libargon2
LOCAL_CPPFLAGS += -fexceptions

LOCAL_C_INCLUDES := \
    $(LOCAL_PATH) \
```

```
    $(LOCAL_PATH)/include \

LOCAL_SRC_FILES := \
    src/argon2.c \
    src/core.c \
    src/blake2/blake2b.c \
    src/encoding.c \
    src/ref.c \
    src/thread.c \

include $(BUILD_SHARED_LIBRARY)
```

编译

```
ndk-build NDK_PROJECT_PATH=. NDK_APPLICATION_MK=Application.mk
```