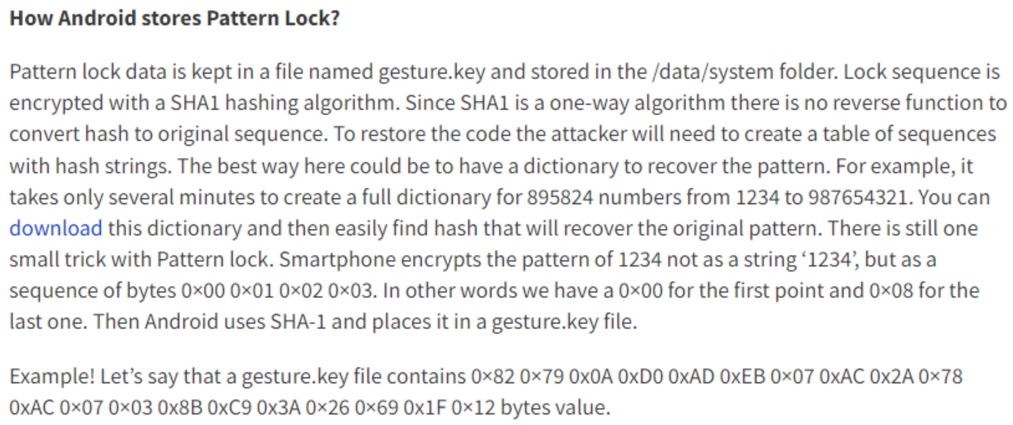
rENTAS CTF WriteUp

By: Elyas Asmad

Mobile (DFIR)

- This challenge provides us with a full incident report (2773 pages) of a mobile phone (Lenovo P70).
- This challenge's flag is the phone password itself.

1. We must know where does Android store the lockscreen password in the file system.



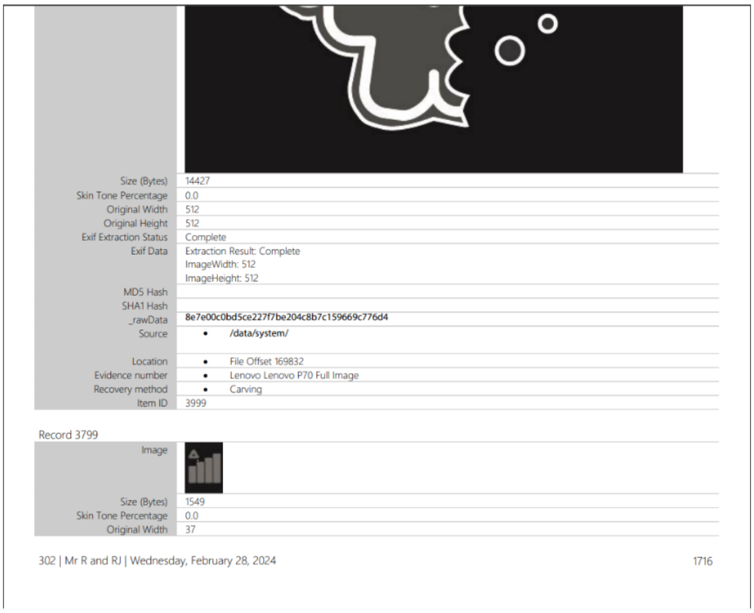
How Android stores Pattern Lock?

Pattern lock data is kept in a file named gesture.key and stored in the /data/system folder. Lock sequence is encrypted with a SHA1 hashing algorithm. Since SHA1 is a one-way algorithm there is no reverse function to convert hash to original sequence. To restore the code the attacker will need to create a table of sequences with hash strings. The best way here could be to have a dictionary to recover the pattern. For example, it takes only several minutes to create a full dictionary for 895824 numbers from 1234 to 987654321. You can download this dictionary and then easily find hash that will recover the original pattern. There is still one small trick with Pattern lock. Smartphone encrypts the pattern of 1234 not as a string '1234', but as a sequence of bytes 0×00 0×01 0×02 0×03. In other words we have a 0×00 for the first point and 0×08 for the last one. Then Android uses SHA-1 and places it in a gesture.key file.

Example! Let's say that a gesture.key file contains 0×82 0×79 0x0A 0xD0 0xAD 0xEB 0×07 0xAC 0x2A 0×78 0xAC 0×07 0×03 0x8B 0xC9 0x3A 0×26 0×69 0x1F 0×12 bytes value.

From this reference, it shows that Android kept them inside `/data/system` folder.

2. By going through all the possibilities of `/data/system` occurrences, we have found this one that is suspiciously being tampered as it shows some font inconsistency.



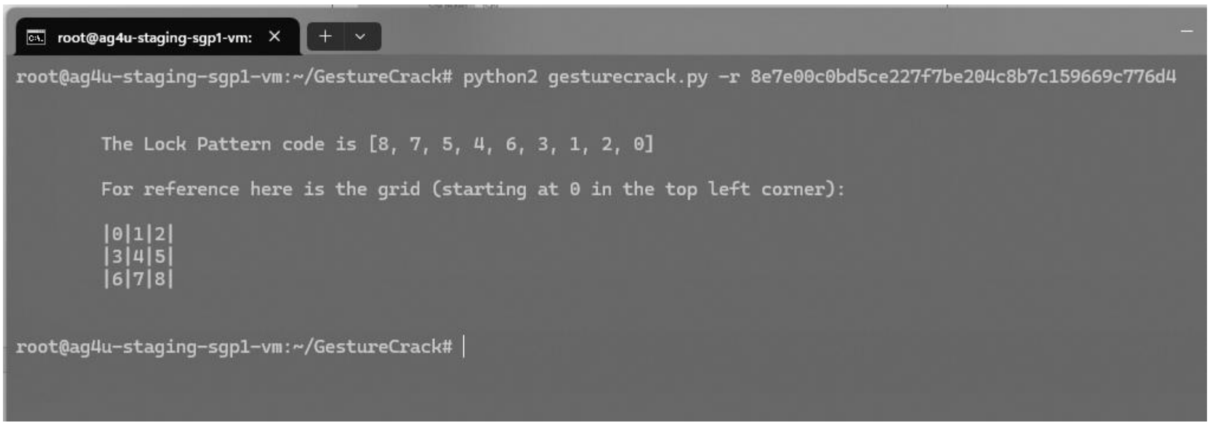
Size (Bytes)	14427
Skin Tone Percentage	0.0
Original Width	512
Original Height	512
Exif Extraction Status	Complete
Exif Data	Extraction Result: Complete ImageWidth: 512 ImageHeight: 512
MD5 Hash	
SHA1 Hash	
_rawData	8e7e00c0bd5ce227f7be204c8b7c159669c776d4
Source	• /data/system/
Location	• File Offset 169832
Evidence number	• Lenovo Lenovo P70 Full Image
Recovery method	• Carving
Item ID	3999

Record 3799

Image	
Size (Bytes)	1549
Skin Tone Percentage	0.0
Original Width	37

302 | Mr R and RJ | Wednesday, February 28, 2024 1716

3. The _rawData property in this particular item seems to be a hash. We can try to crack it using this tool (https://github.com/KieronCraggs/GestureCrack).



```
root@ag4u-staging-sgp1-vm:~/GestureCrack# python2 gesturecrack.py -r 8e7e00c0bd5ce227f7be204c8b7c159669c776d4


        The Lock Pattern code is [8, 7, 5, 4, 6, 3, 1, 2, 0]

        For reference here is the grid (starting at 0 in the top left corner):

        |0|1|2|
        |3|4|5|
        |6|7|8|


root@ag4u-staging-sgp1-vm:~/GestureCrack#
```

Flag: **RWSC{875463120}**