BRUTE FORCE IN COMPUTER CRIMINALISTICS

Kolisa Yaroslav[1]

DOI: https://doi.org/10.30525/978-9934-571-89-3_57

In Ukrainian realities, it is not uncommon to designate locked smartphones for computer forensic expertise. At the same time, the initiator of the research does not have information about the unblocking of the research object. In the absence of specialized hardware and software for selection of password the decision of the forensic expertise is complicated.

One solution to the problem of a locked smartphone, without of password information, is its selection. It is worth mentioning the professionals who use the brute force method. This method can help with checking the cryptographic stability of the password. And given its features, the password will be considered reliable if other methods do not give a faster result.

Now let's understand what is brute force and how can it help a computer criminalist.

Brute force – a method for hacking various accounts by selecting a login and password. Its essence lies in the automated overview of all valid password combinations in the account in order to identify the correct [1].

That is, if you adapt this method to research a smartphone, then an automatched overview of all combinations will be performed. The expert does not need to be executed manually. Of course there are a number of shortcomings in this method. The main thing is the time. About four and a half days can be spent to check all four significant combinations of passwords from “0000” to “9999” [2]. For more combinations, the term increases, which is not appropriate.

In this paper, smartphones are investigated, which are protected by four considerable PIN codes. For example, 2 smartphones were used: Lenovo P1ma40 (Android 5.1) and Sony Xperia XA(F3112) (Android 6.0).

Next, the question arises about the hardware device, which will perform an auto-matched overview of combinations. After analyzing web resources, I decided to stay on Arduino.

Arduino is an open-source electronics platform based on easy-to-use hardware and software. Arduino boards are able to read inputs – light on a sensor, a finger on a button, or a Twitter message – and turn it into an output – activating a motor, turning on an LED, publishing something online. You can tell your board what to do by sending a set of instructions to the microcontroller on the board. To do so you use the Arduino programming language, and the Arduino Software (IDE) [3].

Among all the variety of boards, for the set task are suitable: Arduino Leonadro or Arduino Micro. These models have a microcontroller ATmega32u4 with built-in

[1] Poltava Scientific-Research Forensic Center
Ministry of Internal Affairs of Ukraine, Ukraine

USB connection support. This allows you to recognize your computer as an HID device (a mouse or keyboard) [4].

Arduino boards, Arduino IDE software, microUSB-USB cable and OTG cable are enough to perform brute force [5; 6].

For more efficient use, you need to connect to Arduino, for example, a 7-segment display. This is done to see the combinations that are entered [7]. In addition, after entering the correct password, Arduino will not stop and continue to enter. That is, you must also fix the correct result after unlocking. One of the options is video fixation on the camera. Even suitable for this webcam [8].

As a result of testing on smartphones, a positive result was obtained. Arduino Micro picked up passwords by brute force method.

Thus, the brute force method can solve most cases in the expert practice of unlocking smartphones without time spent with the request of the initiator of the research.

References:

1. Brute force. – Retrieved from: https://www.anti-malware.ru/threats/brute-force (accessed 19 March 2019).

2. Brutfors PIN-kodov iPhone po USB – "Khaker" [Brutfors iPhone Pins for USB – Hacker]. Retrieved from: https://xakep.ru/2015/03/18/ios-pincodes/ (accessed 18 March 2019).

3. Arduino – Introduction. Retrieved from: https://www.arduino.cc/en/Guide/Introduction# (accessed 18 March 2019).

4. Arduino Micro / Apparatnaya platforma Arduino [Arduino Micro / Hardware platform Arduino]. Retrieved from: http://arduino.ru/Hardware/ArduinoMicro (accessed 19 March 2019).

5. Podklyucheniye Arduino i nastroyka / AlexGyver Technologies [Arduino connection and setup / AlexGyver Technologies]. URL: https://alexgyver.ru/arduino-first/ (accessed 19 March 2019).

6. InfoSecSee: Brute forcing Android PIN's with an Arduino and Authentication Weakness. Retrieved from: http://blog.infosecsee.com/2014/01/brute-forcing-android-pins-with-arduino.html (accessed 19 March 2019).

7. Arduino podklyucheniye displeya na TM74HC595 / AlexGyver Technologies [Arduino display connection on TM74HC595 / AlexGyver Technologies]. Retrieved from: https://alexgyver.ru/tm74hc595_display/ (accessed 19 March 2019).

8. Brutforsim EFI s Arduino / Khabr [Brutforsim EFI with Arduino / Habr]. Retrieved from: https://habr.com/ru/post/240291/ (accessed 19 March 2019).