PatternListener: Cracking Android Pattern Lock Using Acoustic Signals

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

1 Summary

Pattern unlocking of the mobile phones is widely used and most famous unlocking system among the mobile users, as it is considered safer than the pin code lock. Software and hardware isolation makes the traditional attacks against pattern lock difficult to infer the pattern lock. However certain shared hardware resources, such as accelerometer, camera, microphone, and GPS may open a door to infer attacks agaist pattern lock. The paper proposes novel acoustic attack, called "pattern listener", which enables cracking of pattern lock, by using inter-perceptible acoustic signals. The base of this attack is that the fingertip on the mobile screen reflects nearby signals, and these signals embed the fingertip motion information related to the unlock pattern. When victim starts to draw the pattern, Patternlistener generates audio and it plays it using the speakers. Then microphone is used to record these acoustic signals and the remote server then processes these signals. The authors developed different algorithms for pattern detection. Patternlistener constructs different lines according to the trajectories and deduce (coherent detection together with static components) a lock pattern. They implemented Patternlistener on off the shelf devices and they claim that Patternlistener can successfully exploit over 90% patterns within five attempts.

2 Contribution

Paper proposes Patternlistener, a new pattern lock vulnerability, which uses shared hardware resources, such as speakers and microphone to infer the lock pattern. And they claim that something link this has never been proposed before. They developed several algorithms for Patternlistener. They have implemented the prototype of the Patternlistener on different devices.

3 Strengths

One of the important strength is that Patternlistener can infer unlock patterns of large number of devices simultaneously. It is robust to the environmental interference and changes in drawing speed, gestures and different screen sizes. Also complicated code doesn't affect Patternlistener detection. The results demonstrate that it can crack over 90% of 130 patterns within five attempts. Also I like the pattern generation process described in the paper.

4 Limitations

One of the important weakness that I think of is deployment of Patternlistener. T detect the pattern the must be deployed to the victim in some way (which I think is hard). 2-D gesture detection is not possible using Patternlistener. Also, as authors mentioned, the attack fails in case of randomized pattern grid. Also, I think that the accuracy of detection kind of depends on the hardware (But I think modern devices have good speakers and mic, so this may not be the disadvantage in that case).

5 Future Work

Attack can be modified to support 2-D gesture tracking using speakers and microphone. Attack can be improved (maybe) with the combination of other attacks (such as smudge attack).

References

[1] Man Zhou, Qian Wang, Jingxiao Yang, Qi Li, Feng Xiao, Zhibo Wang, Xiaofeng Chen *Pattern-Listener: Cracking Android Pattern Lock Using Acoustic Signals*, CCS'18