# Article information:

Using a Blocklist to Improve the Security of User Selection of Android Patterns | USENIX  
<https://www.usenix.org/conference/soups2021/presentation/munyendo>

# Article summary:

1. Android patterns are a popular method for unlocking smartphones, but many users choose easily guessable patterns.

2. The usage of blocklists can improve the security of user-chosen patterns by disallowing common patterns, a feature currently unavailable on Android but used by Apple during PIN selection.

3. A user study found that even the smallest blocklist (12 patterns) had benefits, reducing a simulated attacker's success rate after 30 guesses from 24% to 20%, and blocking 100 patterns was recommended for a good balance between usability and security.

# Article rating:

May be slightly imbalanced: The article presents the information in a generally reliable way, but there are minor points of consideration that could be explored further or claims that are not fully backed by appropriate evidence. Some perspectives may also be omitted, and you are encouraged to use the research topics section to explore the topic further.

# Article analysis:

The article "Using a Blocklist to Improve the Security of User Selection of Android Patterns" presents a study conducted by researchers from The George Washington University, Ruhr University Bochum, and the United States Navy. The study explores the use of blocklists to improve the security of user-chosen patterns on Android devices.

The authors begin by highlighting the popularity of Android patterns as a method for unlocking smartphones, despite evidence suggesting that many users choose easily guessable patterns. They propose using blocklists to disallow common patterns, a feature currently unavailable on Android but used by Apple during PIN selection.

The study involved testing five different blocklist sizes on participants' smartphones (n = 1006) and comparing them to a control treatment. The authors found that even the smallest blocklist (12 patterns) had benefits, reducing a simulated attacker's success rate after 30 guesses from 24% to 20%. The largest blocklist (581 patterns) reduced the percentage of correctly guessed patterns after 30 attempts down to only 2%.

In terms of usability, blocklists had limited negative impact on short-term recall rates and entry times, with reported SUS values indicating reasonable usability when selecting patterns in the presence of a blocklist.

Overall, the study provides valuable insights into how blocklists can improve the security of user-chosen patterns on Android devices. However, there are some potential biases and limitations to consider.

Firstly, the study only tested one type of attack scenario - a simulated attacker guessing patterns - which may not reflect real-world attacks. Additionally, it is unclear whether participants were representative of typical smartphone users or if they had above-average security awareness.

Furthermore, while the authors acknowledge that larger blocklists may negatively impact usability, they do not explore potential trade-offs between security and usability in more detail. It would be interesting to see how users' perceptions of security and ease-of-use change as blocklist size increases.

Finally, the authors do not discuss potential risks associated with blocklists, such as the possibility of false positives or the need for regular updates to keep up with evolving attack methods.

In conclusion, while the study provides valuable insights into how blocklists can improve the security of user-chosen patterns on Android devices, there are some potential biases and limitations to consider. Further research is needed to explore trade-offs between security and usability and to assess potential risks associated with blocklists.

# Topics for further research:

* Trade-offs between security and usability in Android pattern selection
* Real-world attack scenarios on Android pattern selection
* User demographics and security awareness in Android pattern selection studies
* Risks associated with false positives in Android pattern blocklists
* Updating Android pattern blocklists to keep up with evolving attack methods
* Comparison of blocklist effectiveness with other Android pattern security measures

# Report location:

<https://www.fullpicture.app/item/f5897e364f744361047d6b2265d41602>