# Article information:

Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns | Annual Computer Security Applications Conference
<https://dl.acm.org/doi/10.1145/3427228.3427252>

# Article summary:

1. Double Patterns (DPatts) is a proposed advancement on Android unlock patterns that maintains the core design but instead of selecting a single pattern, a user selects two patterns entered one-after-the-other super-imposed on the same 3x3 grid.

2. DPatts are more secure than traditional patterns based on standard guessability metrics, more similar to that of 4-/6-digit PINs, and even more difficult to guess for a simulated attacker.

3. Participants found the DPatts interface quite usable, with high recall retention and comparable entry times to traditional patterns. Current Android pattern users reported high perceptions of security and usability in responses to open- and closed-questions.

# Article rating:

Appears strongly imbalanced: The article is written in a biased or one-sided way, and the information it provides is not trustworthy enough to be considered a reliable source. You should consult other sources to find reliable information on the presented issues.

# Article analysis:

The article titled "Double Patterns: A Usable Solution to Increase the Security of Android Unlock Patterns" proposes a new method for securing Android devices by introducing Double Patterns (DPatts). The authors claim that DPatts are more secure than traditional patterns and have high usability. However, the article has several potential biases and missing points of consideration.

One-sided reporting is evident in the article as it only focuses on the benefits of DPatts and does not explore any potential drawbacks or limitations. For instance, the authors do not discuss whether DPatts may be more difficult for users with certain disabilities or impairments to use. Additionally, there is no discussion of how DPatts may impact battery life or device performance.

The claims made in the article are largely unsupported as there is no evidence presented to support them. For example, the authors state that DPatts are more secure than traditional patterns based on standard guessability metrics but do not provide any data to back up this claim. Similarly, they claim that users find DPatts interface quite usable but do not provide any specific feedback from participants to support this assertion.

The article also lacks exploration of counterarguments or alternative solutions. For example, while DPatts may be an improvement over traditional patterns, it is unclear if they are superior to other methods such as biometric authentication or two-factor authentication.

There is also promotional content present in the article as the authors recommend adding DPatts as an advancement to Android patterns without considering any potential risks or drawbacks. It is important to note that any new security measure can introduce new vulnerabilities and risks that need to be carefully considered before implementation.

Overall, while the concept of Double Patterns may have merit, this article lacks critical analysis and presents a one-sided view of its potential benefits without exploring its limitations or drawbacks. Further research and analysis are needed before recommending its implementation as a security measure for Android devices.

# Topics for further research:

* Accessibility considerations for Android device security measures
* Impact of security measures on battery life and device performance
* Comparison of DPatts to other authentication methods such as biometrics and two-factor authentication
* Potential vulnerabilities and risks introduced by new security measures
* User feedback and satisfaction with DPatts compared to traditional patterns
* Studies on the effectiveness of guessability metrics in evaluating the security of authentication methods.

# Report location:

<https://www.fullpicture.app/item/31b704c4598b85ed74687b879e42ade1>