# Article information:

[1807.00459] How To Backdoor Federated Learning  
<https://arxiv.org/abs/1807.00459>

# Article summary:

1. Federated learning enables multiple participants to construct a deep learning model without sharing private training data.

2. An attacker can introduce hidden backdoor functionality into the joint global model, such as ensuring an image classifier assigns an attacker-chosen label to images with certain features.

3. A new model-poisoning methodology based on model replacement is designed and evaluated, which can cause the global model to immediately reach 100% accuracy on the backdoor task.

# Article rating:

Appears moderately imbalanced: The article provides some useful information, but is missing several important points or pieces of evidence that would be required to present the discussed topics in a balanced and reliable way. You are encouraged to seek a more balanced perspective on the presented issues by exploring the provided research topics and looking at different information sources.

# Article analysis:

The article “How To Backdoor Federated Learning” provides a detailed overview of how attackers can introduce hidden backdoor functionality into federated learning models. The article is well written and provides a comprehensive explanation of the attack methodology, as well as its evaluation under different assumptions for standard federated-learning tasks. However, there are some potential biases in the article that should be noted. For example, the article does not explore any counterarguments or present both sides of the issue equally; instead it focuses solely on how attackers can exploit federated learning models for malicious purposes. Additionally, there is no discussion of possible risks associated with this type of attack or any mention of potential solutions to mitigate these risks. Furthermore, while the article does provide evidence for its claims, it could benefit from additional evidence and research to further support its conclusions. In conclusion, while this article provides a thorough overview of how attackers can exploit federated learning models for malicious purposes, it could benefit from more balanced reporting and additional evidence to further support its claims.

# Topics for further research:

* Mitigating risks of backdoor attacks in federated learning
* Countermeasures for backdoor attacks in federated learning
* Security implications of backdoor attacks in federated learning
* Research on backdoor attacks in federated learning
* Evidence for backdoor attacks in federated learning
* Solutions for backdoor attacks in federated learning

# Report location:

<https://www.fullpicture.app/item/36cf3db135bb37975db818450153bfe6>