



Hell vector created by upklyak - www.freepik.com

Machine Learning in Adversarial Settings

Maximilian Noppel
Mittwoch, 18.Mai 2022
19:30 Uhr online (siehe Wiki)

Beschreibung. Machine Learning zu verwenden ist inzwischen einfacher den je. Dennoch gibt es gewisse Sicherheitsproblemchen auf die man bei der Anwendung achten sollte. Die bekanntesten, *Adversarial Examples*, sind sicherlich vielen ein Begriff, es gibt aber noch viele weitere Angriffvektoren und Angreiferziele. In diesem Talk werde ich einige dieser Angriffsszenarios auf Machine Learning vorstellen.

