Seitenkanalangriff

Rubrik: IT-Sicherheit

Ein Seitenkanalangriff gewinnt Informationen aus Begleiterscheinungen einer Berechnung statt direkt aus ihrem Ergebnis.

Ein Seitenkanalangriff gewinnt Informationen aus Begleiterscheinungen einer Berechnung statt direkt aus ihrem Ergebnis. Dazu können Laufzeit, Stromverbrauch oder elektromagnetische Abstrahlung gehören. Besonders kryptografische Implementierungen können dadurch unbeabsichtigt Geheimnisse preisgeben. Gegenmaßnahmen müssen deshalb auch das Verhalten der Hardware und Software berücksichtigen.