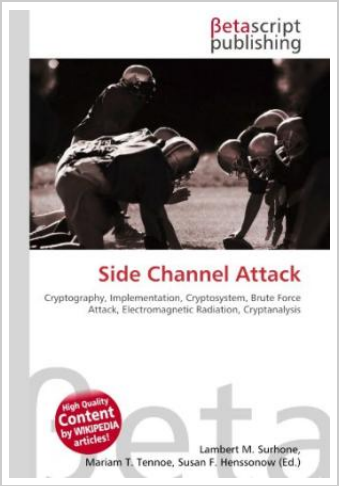

Side Channel Attack

By Lambert M. Surhone

Betascript Publishers Feb 2010, 2010. Taschenbuch. Condition: Neu. Neuware - High Quality Content by WIKIPEDIA articles! In cryptography, a side channel attack is any attack based on information gained from the physical implementation of a cryptosystem, rather than brute force or theoretical weaknesses in the algorithms (compare cryptanalysis). For example, timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information which can be exploited to break the system. Many side-channel attacks require considerable technical knowledge of the internal operation of the system on which the cryptography is implemented. Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically called side-channel attacks: see social engineering and rubber-hose cryptanalysis. For attacks on computer systems themselves (which are often used to perform cryptography and thus contain cryptographic keys or plaintexts), see computer security. 88 pp. Englisch.

Reviews

The best pdf i possibly go through. it was writtern quite properly and useful. Once you begin to read the book, it is extremely difficult to leave it before concluding.

-- ***Miss Sienna Fay Jr.***

This composed pdf is great. It usually will not cost too much. I am very easily can get a pleasure of reading a composed book.

-- ***Luis Klein***