Side-Channel Attack

Return to Glossary

Side-Channel Attack is any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself (e.g. cryptanalysis and software bugs). Timing information, power consumption, electromagnetic leaks or even sound can provide an extra source of information, which can be exploited.

Some side-channel attacks require technical knowledge of the internal operation of the system, although others such as differential power analysis are effective as black-box attacks. The rise of Web 2.0 applications and Software as a Service (SaaS) has also significantly raised the possibility of Side-Channel Attack on the web, even when transmissions between a web browser and server are encrypted (e.g. through Hypertext Transport Protocol Secure (HTTPS) or Wireless Fidelity (Wi-Fi) Encryption).

Source: https://en.wikipedia.org/wiki/Side-channel_attack