Oksana Cherednichenko
A.A. Baranov, research supervisor
T.I. Morozova, language adviser
SHEI “National Mining University”, Dnipropetrovsk

Side-channel Attack

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, electromagneticleaks or even sound can provide an extra source of information which can be exploited to break the system. Some side-channel attacks require technical knowledge of system internal operation on which the cryptography is based. Differential power analysis is effective as black-box attack. The most powerful side channel attacks are also based on statistical methods pioneered by Paul Kocher .

Attempts to break a cryptosystem by deceiving or coercing people with legitimate access are not typically called side-channel attacks: social engineering and rubber-hose cryptanalysis. To attacks computer systems computer security is used. The rise of 2.0 web applications and software-as-a-service has also significantly increased the possibility of side-channel attacks on the web, even when transmissions between a web browser and server are encrypted (e.g., through HTTPS or WiFi encryption).

General classes of side-channel attack include:

- Timing attack — attacks based on measuring time spent on various computations.
- Power monitoring attack — attacks which make use varying power consumption by the hardware during computation.
- Electromagnetic attacks — attacks based on leaked electromagnetic radiation which can directly provide plaintexts and other information. Such measurements can be used to infer cryptographic keys using techniques equivalent in power analysis, or can be used in non-cryptographic attacks, e.g. TEMPEST (aka van Eck phreaking or radiation monitoring) attacks.
- Acoustic cryptanalysis — attacks which exploit sound produced during computation (rather like power analysis).
- Differential fault analysis in which secrets are discovered by introducing faults in computation.
- Data remanence in which sensitive data are read after supposedly having been deleted.