Cold Boot Attack

Return to Glossary

Cold Boot Attack or a platform reset attack, is a type of side channel attack in which an attacker with physical access (see Physical Security) to a computer performs a memory dump of a computer's Random Access Memory (RAM) by performing a hard reset of the target machine. Typically, Cold Boot Attacks can retrieve encryption keys from a running Operating System (OS) for malicious and/or criminal investigative reasons. The attack relies on the Data Remanence property of Dynamic Random Access Memory (DRAM) and Static Random Access Memory (SRAM) to retrieve memory contents that remain readable in the seconds to minutes after power has been removed.

An attacker with physical access to a running computer typically executes a Cold Boot Attack by cold-booting the machine and booting a lightweight operating system from a removable disk to dump the contents of pre-boot physical memory to a file. An attacker is then free to analyze the data dumped from memory to find sensitive data, such as the keys, using various forms of key finding attacks. Since Cold Boot Attacks target random-access memory, Full-Disk Encryption (FDE) schemes, even with a trusted platform module installed are ineffective against this kind of attack. The problem is fundamentally a hardware (insecure memory) and not a software issue. However, malicious access can be prevented by using Physical Security and using modern techniques to avoid storing sensitive data in random-access memory.

Source: https://en.wikipedia.org/wiki/Cold_boot_attack