TRESOR

Return to Glossary

TRESOR is a software approach that seeks to resolve this insecurity by storing and manipulating encryption keys almost exclusively on the Central Processing Unit (CPU) alone, and in Registers accessible at Protection Rings **Ring 0** (the highest privilege level) only—the exception being the brief period of initial calculation at the start of a session. This ensures that encryption keys are almost never available via user space or following a cold boot attack. **TRESOR** is written as a kernel patch that stores encryption keys in the x86 debug registers, and uses on-the-fly round key generation, atomicity, and blocking of usual **`ptrace`** access to the debug registers for security.

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