Argonne NATIONAL LABORATORY | Nuclear Engineering Division

Key Keepaway

Securing a secret key by keeping its fragments in motion.

The Problem

When physical or electronic intrusion is detected, a secret, electronic key often needs to be erased. It is difficult to do this quickly enough & reliably (given data remanence), especially for large (256 byte) keys needed for high security encryption & equipment.

The Solution

Portions of the secret key bounce around in a microprocessor circuit or microprocessor wheel in a complex, unpredictable manner.

Quantum noise is used (or else a chaotic, non-linear, recursive equation) to direct where portions of the key go. Neither the central microprocessor nor the designer/programmer knows where the key fragments are at any given time.

To reassemble the key, the CPU issues a reassemble command and waits for the key portions to show up randomly, typically 0.5 seconds later vs. << 1 microsecond to destroy the key.

Key storage is dynamic so information is lost mid-transfer when erasure is called for. The microprocessor also has a non-graceful shutdown behavior on power loss.

Data remanence is much less of a risk with this dynamic, chaotic approach.

The Vulnerability Assessment Team

The award-winning Vulnerability Assessment Team (VAT) at Argonne National Laboratory (formerly at Los Alamos from 1992-2007) provides security consulting, training, vulnerability assessments, and R&D to a wide range of sponsors. Examples include DoD, DOE/NNSA, U.S. Department of State, IAEA, Euratom, intelligence agencies, NGOs, and private companies.

The VAT resources include top secret security clearances, a unique Vulnerability Assessment Laboratory, 3200 square feet of laboratories and office space including 2000 square feet of VTR laboratories for classified work, a rapid prototyping microprocessor shop, and access to 2 SCIFs (with a third one under construction). The VAT has successfully completed $25 million of classified and unclassified projects since 1992.

Argonne NATIONAL LABORATORY

CONTACT > Roger G. Johnston, Ph.D., CPP | 630-252-6168 | rogerj@anl.gov | Nuclear Engineering Division | www.anl.gov