

54th Meeting of the IFIP WG10.4 "Dependable Computing and Fault Tolerance"
Workshop on Challenges and Directions in Dependability, Girdwood, AK, June 28-29, 2008

A Creedence in HW-Matter Revival *

Jean Arlat



** Rockability :-)*₁

About Trends

- Recent advances in hardware technologies
—> dramatic development of embedded systems and unprecedented spread of pervasive computerized appliances and applications
- Tracks towards nanoscale computing
 - ◆ Top Down (*More Moore*) — Shrinking CMOS technology devices
Increasing impact of variations in features
 - ◆ Bottom up (*Beyond Moore*) — Self-assembling nanoscale elements
Signal amplification, selective control, ...
- In both cases, increased **unreliability**, higher **susceptibility** and even **unpredictability**, are forecasted to be at the corner...

Fault categories

- **Soft errors (transients): A great deal of efforts made and significant achievements** — e.g., invited talk by Pia Sanda about IBM POWER6™ microprocessor during Workshop on Nanocomputing at DSN08.
- **Unreliability of basic devices/components**
—> Low production yield => live with partially defective chips?
- **Security protections implemented in HW (better control)**
 - ◆ Side channel attacks — information leakage
 - ◆ Differential fault analysis — out-of range conditions, including fault injection ;-)
 - ◆ Exploitation of built-in testability features: Scan-based testing devices — An Embedded Trojan horse?
- **New fault models related to emerging bottom-up technologies**

Researchers Find Way to Steal Encrypted Data

By JOHN MARKOFF



SAN FRANCISCO — A group led by a Princeton University computer security researcher has developed a simple method to steal encrypted information stored on computer hard disks.


The technique, which could undermine security software protecting critical data on computers, is as easy as chilling a computer memory chip with a blast of frigid air from a can of dust remover. Encryption software is widely used by companies and government agencies, notably in portable computers that are especially susceptible to theft.

The development, which was described on the group's Web site Thursday, could also have implications for the protection of encrypted personal data from prosecutors.

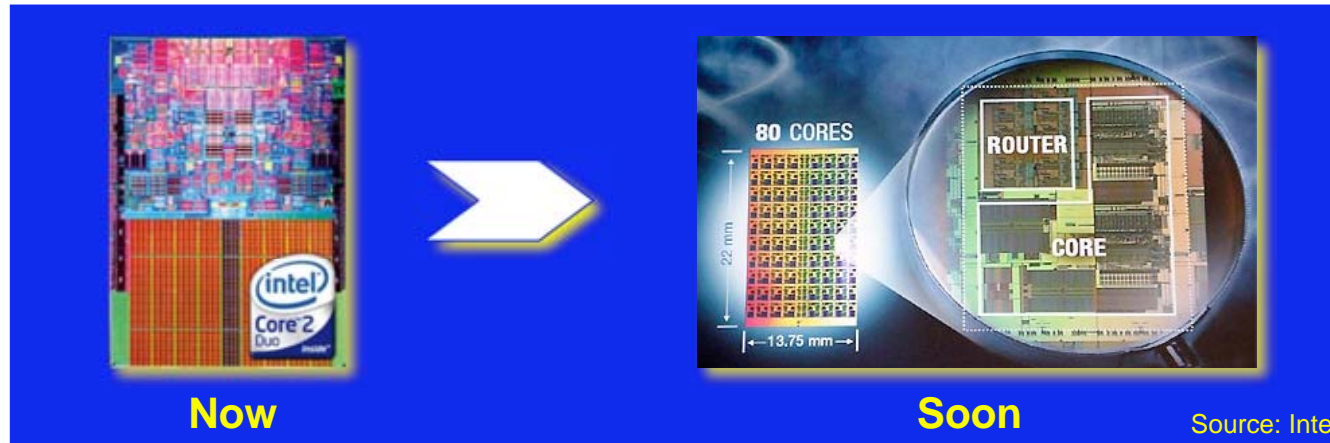
The move, which cannot be carried out remotely, exploits a little-known vulnerability of the dynamic random access, or DRAM, chip. Those chips temporarily hold data, including the keys to modern data-scrambling algorithms. When the computer's electrical power is shut off, the data, including the keys, is supposed to disappear.

...

Some “New” Paradigms

- Depart from the basic “Frequency & Size” rationale (power dissipation issues)
- From “100% Correct” to “Less than Perfect” chips
- From device-level mitigation techniques to architectural-level resilience techniques
- Memory: Static and on-line degradable-reconfigurable chips
- Processor:  ROI in computation power gain wrt area and power dissipation for most advanced “X-scalar” architectures
—> “vectorial” multi-core arrays, networks-on-chips, etc.

From Multi-Cores Architectures To Multi-Multi-Cores Architectures



- Multi-Core: ↗ performance while coping with power dissipation issues (very high clock frequency)
- Still, ↘ transistor size for including many of such cores
—> significant % of defective cores ($\approx 10\%$ and even more)
- Current context:
 - ◆ Chips are sorted according to frequency
 - ◆ Single core processor = “Downgraded” dual core circuits ...
- How to go further: on-line reconfiguration to cope with faults?

A Strategic "Niche" and an Opportunity!

■ For research activities:

- ◆ Bridge the gap between hardware-level and system-level issues
- ◆ Extend the applicability of our core-skills and develop beyond that
- ◆ Embedded systems are open systems that are impacted by the full range of threats (including attacks)

■ More impact on basic components that underly our systems

■ Extend the reachability of DSN

—> Workshop on Dependable and Secure Nanocomputing

- ◆ Raised interest and was well-attended
- ◆ Proposal from IEEE Int. On-Line Testing Symposium to be co-located with DSN-2009 is another good sign...

■ A rationale for a WG 10.4 Workshop... ;-)