Secure silicon: Enabler for the Internet of Things

Walden C. Rhines
Mentor Graphics

Abstract

As electronic system hackers penetrate deeper—from applications to embedded software to OS to silicon—the impact of security threats is growing exponentially. Viruses and malware in the operating system, or application layer, are major concerns, but only affect a portion of users. In contrast, even small malicious modifications or compromised performance in the underlying silicon can devastate system security for all users. Growth of the Internet of Things magnifies the impact of the security problem by orders of magnitude.

Since hardware is the root of trust in an electronic product, EDA companies will be increasingly pressured to solve the silicon security problems for their customers. This requires a new paradigm in silicon design creation and verification. The traditional EDA role is to design and then verify that the silicon does what it is supposed to do. Creating secure silicon, however, requires that verification ensure that the chip does nothing that it is NOT supposed to do.

The industry is at the first stage of Secure Silicon awareness; it's going to become big business as future events unfold. Join Wally Rhines as he examines the growing threats to silicon security and EDA's possible solutions.