Hardware and Software Design Security; It’s All in the Mix

Vandana Lokeshwar, element14, www.element-14.com

Western high-tech businesses know they must continuously deliver innovative ideas and unique features to their customers, to protect market share and brand value. This situation makes the defense of intellectual property against threats such as reverse engineering, cloning and tampering extremely important. Careful attention to device-level security features is an important aspect of design.

Today’s design techniques, which aim to maximize integration for purposes such as reducing size and cost while maximizing reliability, tend to consolidate much of the design’s unique features in components such as microcontrollers and FPGAs, which are relatively vulnerable to interception or interference with program data stored in memory.

Techniques used to prevent access to such data can include measures to prevent physical probing, encryption of the data, or mechanisms to destroy the data if an unauthorized attempt at access is detected. Xilinx, for example, uses features such as configuration-data protection, hidden bitstream, and active defense in its Extended Spartan-3A FPGAs and CoolRunner™-II CPLDs targeting high-volume product designs. Xilinx has also implemented Device DNA for low-cost hardware and software IP protection. Here, a unique 57-bit Device DNA number is used with a customer-defined security algorithm to generate an active value. The active value is compared to a pre-stored check value to determine whether design functionality can proceed.

In higher-value designs using more powerful and complex FPGAs, encryption of the configuration bitstream using an industry standard such as 256-bit AES encryption/decryption with a battery-backed key, may be a viable solution. This capability is built into in devices such as the Xilinx Virtex™-5 or Altera Cyclone® III families. Further measures to prevent interception of the encryption key can include burying the key under layers of metal to resist physical attacks such as de-packaging of the die. Architectures such as Cyclone III also use techniques such as hiding the key by distributing it among other logic, and features to erase the key if tampering is detected.

Based on Atmel’s AT90SO secureAVR® microcontrollers, products such as AT90SO4 and VaultIC200 solve the problems of cloning, counterfeiting and IP stealing by offering cryptography functionality, secure data storage and industry-standard interfaces that serve as a tamper- resistant authenticity seals.

Chip-erase modes for auto-erasing of data memory are also evident in many microcontrollers from vendors such as Microchip, Freescale, and TI. Unlike most FPGAs, a microcontroller has no configuration bitstream to access. This means attackers are more likely to attempt direct physical access to the on-chip memory.

As well as de-packaging, other exploits can include attempts to disable any memory protection features by generating over- or under-voltage events at the power supply pins or by applying sequences of glitches to I/Os. Microcontrollers, and, indeed, FPGAs built using one-time programmable (OTP) memory technologies are generally regarded as offering greater security to reverse engineering or tampering. However, this comes at the expense of a loss of flexibility.

As any security specialist will confirm, access prevention can never be absolute; but relative security can be achieved by imposing high costs on the would-be attacker, in terms of the necessary equipment and time necessary to access the data. Alongside device-level security, therefore, being the first to market with the next new idea is also a valuable part of the security “mix”.