Security

CIRKEYTRY

Ramping security protocols are a necessary measure to safeguard against intruders. Dave Locke looks at an encryption option in defence

Today's electronic systems – both military and civil – are equipped with an ever-increasing raft of security measures.These incorporate not just secure hardware, but also require the use of a rapidly-evolving set of complex encryption algorithms.

And yet, all of these features can be rendered useless if an unauthorised individual (or organisation) gains access to the system's security key codes. The choice of storage medium for such keys, and of techniques for protecting them, is therefore a critical decision in ensuring the overall security of the system.

System security

A typical secure communications processing system has at its core a complex encryption/ decryption engine implemented either via custom logic (an ASIC or FPGA), or with a more general-purpose microprocessor and custom software defining the encryption algorithm. In most cases, the secure key code is stored in a separate memory chip off-chip from the encryption engine that is powered by a battery, an approach that ensures that the keys are constantly accessible when system power is on, and yet are retained or backed up for long periods when the system power is shut down.

The need to keep the keys off-chip, however, increases the difficulty of securing them against tampering. Most secure encryption systems will include anti-tampering logic that will immediately clear the keys if system tampering has been detected. Such anti-tampering countermeasures are typically implemented with a layered approach, overlapping and integrating a mix of mechanical and electrical techniques.

Integral to devising an effective security system is the choice of storage medium itself. The most obvious choice is to use non-volatile memory such as flash, EEPROM, or permanent storage media such as CDs or DVDs. These systems are inherently able to retain data when system power is shut down, and can be protected with circuitry that erases the keys in the event of tampering.

However, such a system must be exceptionally well designed to resist a determined attack. In the case of flash memory or EEPROM, it might appear that it would be adequate to include logic to assert a "clear" signal to reset individual logic bits to logic '0'. However, the individual memory bits will always retain some amount of charge from their previous state, allowing reverse-engineering techniques to be used to extract the previously stored key code.

Ensuring that all of the information in a non-volatile memory has been completely erased requires multiple writes of all '0's, all '1's, or a checkerboard pattern, a process that typically requires at least 20 clock cycles. The anti-tampering system must therefore at all times retain sufficient power to drive the anti-tamper logic and enable the erasure process. Such a system can be designed with components as simple as a large capacitor to store power, but this power supply itself requires protection against tampering. Moreover, it is not beyond the realms of possibility that 20 clock cycles may not be immediate enough for clearing the memory to defeat sophisticated tamper techniques.

Clearing all traces

Erasing CDs or DVDs also has its own unique set of concerns. The CD or DVD can be destroyed with acids or fire, but for all practical purposes this requires the system operator to anticipate the threat of tampering and act accordingly. Electrical erasure is possible with some formats, but is time consuming, and, as with non-volatile memory, must ensure that no residual data is left on the media.

To solve these problems, several FPGA suppliers have offered encrypted configuration file memory solutions. These provide the benefit of not requiring a battery back up and power management circuitry, since they store the key in non-volatile memory within the FPGA, which provides some inherent barriers to reverse engineering. However, the key code remains in non-volatile storage and, although the reverse engineering and/or obfuscation barriers are somewhat increased, they are not insurmountable with sufficient resources.

Because of the challenges of non-volatile storage, volatile memory is most commonly the solution of choice in applications that require truly robust security. Anti-tamper logic clears the memory if the system is tampered with, and a battery is included to ensure data retention when the system is shut down. Power management circuitry is required to switch between system-powered and battery-powered states, and minimise battery drain.

The pros & cons

Such a solution has its own inherent drawbacks. A clock may be required to refresh the memory, whether the system is powered-up or on battery standby, increasing the drain on the battery. More seriously, recent studies have shown that data stored in DRAM may not be instantaneously lost when power is removed. Research reported by Princeton University Centre for Information Technology Policy has demonstrated that such data may be retained for seconds or even minutes after power-down. This is true even when the memories are removed from their motherboards, allowing algorithms to be used to read back sensitive data.

The ideal solution to this design problem combines a number of features. The system must be able to detect tampering and trigger an erase of the secure key code memory; the memory should be erased as quickly and completely as possible to prevent reconstruction of its contents; and yet the battery lifetime must be long enough to retain the keys throughout power-down, potentially over a period of years.

Of the solutions we have already examined, volatile memories best meet these requirements. They can be erased with a direct action clear signal without the need to generate any clock signals. An active-low clear signal can be used to work with electro-mechanical designs that tie the clear signal to system ground when a tampering event occurs. The use of battery power coupled with a low power memory and power management circuitry can retain codes stored in volatile memory for long periods of time without system power applied.

To operate successfully they require power management circuitry, creating a new hybrid power domain. Whilst it can also be used to power some or all of the anti-tampering logic, it is because of this additional power domain that system designers cannot integrate the secure key code memory and any of the anti-tamper logic into the encryption/decryption engine – whether it is implemented as a microprocessor, ASIC or FPGA. As a result, the system implementation of the volatile memory requires multiple components on the system board.

Moreover, for each component on the system board that stores, reads or writes the secure key code, there is a corresponding increase in susceptibility to a tampering event that could reveal the key itself. In addition, the system operational reliability decreases and manufacturing costs increase with each additional component mounted on the system board.

These problems can be solved by the use of an ASIC, FPGA or microprocessor platform that includes an on-chip encryption/decryption engine and supports volatile memory powered by a separate power domain. Key characteristics of such an integrated device include no external access to the secure key code memory other than the clear signal, built in power management, a separate power domain for the secure key code memory and configurable anti-tamper logic.

In practice

Integrating these functions into a single product optimises system security while improving system reliability and decreasing manufacturing costs. Potential solutions would integrate an encryption engine such as ON Semiconductor's XPressArray-II structured ASIC platform with the secure memory and power management circuits to realise an optimum solution. This kind of development is technically feasible with mature silicon technologies, and requires only the commitment of a supplier to the secure military communications market.

ON Semiconductor | www.onsemi.com

Dave Locke is Mil/Aero Product Manager at ON Semiconductor