Advancing System and Device Security
Using Silicon-Proven Programmable Logic IP

by Paul Bradley, Former DAFCA CTO
edited by Sawblade Ventures, LLC

The global cost of assaults on electronic systems and infrastructure is staggering. Attacks that were once perpetuated by small ad-hoc collections of individuals are now being conducted by well-funded organizations. The most widely publicized events are those executed against various defense, government, utility, and financial sector infrastructures. However, the consumer products market is increasingly affected by device tampering, counterfeit activity, and digital rights and intellectual property theft.

While efforts to secure the electronic systems and data within using a combination of cryptography and secure software are critical, more must be done to prevent tampering, reverse engineering, and unauthorized use. It is through tampering and reverse engineering that many attackers learn enough about a system to expose its weaknesses. Exposed weaknesses may be in hardware or software, or both.

Sawblade Ventures (SbV) solves this problem by allowing system designers to implant small monitors within the electronics system to detect and prevent tampering and reverse engineering.

Perhaps the biggest challenge facing system designers is anticipating the unknown. This problem is compounded by the high cost of development and the potentially devastating and lethal cost of being wrong.

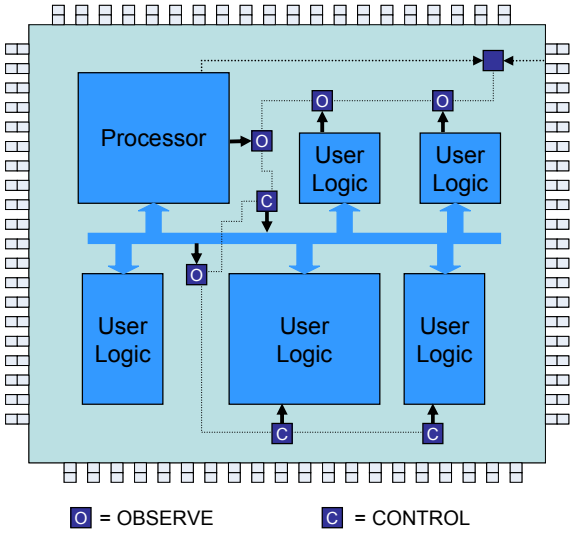

Figure 1: Chip-level monitoring (ASSP, ASIC, FPGA, MCU)

A way to combat such challenges is through a hedge. From a system architecture perspective, this often means using software and programmable logic whenever possible to implement critical functionality. The benefit is that software and programmable logic can be updated to counteract new threats or resolve insufficiencies discovered in the system.

SbV is introducing a novel, programmable-logic approach to significantly improve today's security coverage by improving it at the system level and extending it to the device level. SbV provides synthesizable programmable logic structures and powerful insertion tools to embed programmable monitors within an MCU, ASIC, ASSP, FPGA, or PCBA design. The programmable monitors are inserted during the design phase. The programs to be loaded into the monitors are also designed during the design phase, but new programs can be designed at any point in the

product lifecycle, whether to enhance functionality, improve coverage, or guard against new and unexpected threats. The programs instruct the monitor to look for suspicious behaviors such as:

- Unauthorized JTAG port activity
- Abnormal reset behavior
- Abnormal power cycling and sequencing behavior
- Abnormal performance profiles
- Unauthorized memory accesses including BIOS changes
- Killed processes

The application of these programmable monitors is nearly unlimited , restricted only by the programmable FSM resources provided within.

The programmable monitors operate at-speed and can counteract suspected threats with immediate countermeasures when used in conjunction with SbV's security wrappers. These wrappers enable real-time responses to threats by the following:

- Forcing circuits into a reset state (e.g., communication peripherals, memory controllers)
- Blocking read and/or write access to select memories, memory regions, or peripherals
- Creating obfuscated bus activity or other masking functions
- Wiping out (erasing) sensitive data stored in select memories
- Creating alerts and allowing the system to enter "safe mode" gracefully

The monitoring activity can extend into software. In fact, the solution can be greatly enhanced by combining the programmable monitors with SbV software-based security monitoring functions. The software security monitoring system interacts with the hardware monitors to enable additional functions such as:

- Creating a more secure boot and initialization sequence binding the hardware and software subsystems
- Enabling a constant challenge response handshake to reduce threats from man-in-the-middle attacks or software performance and process abnormalities
- Advancing software analysis by exchanging performance and behavior metrics computed in hardware monitors

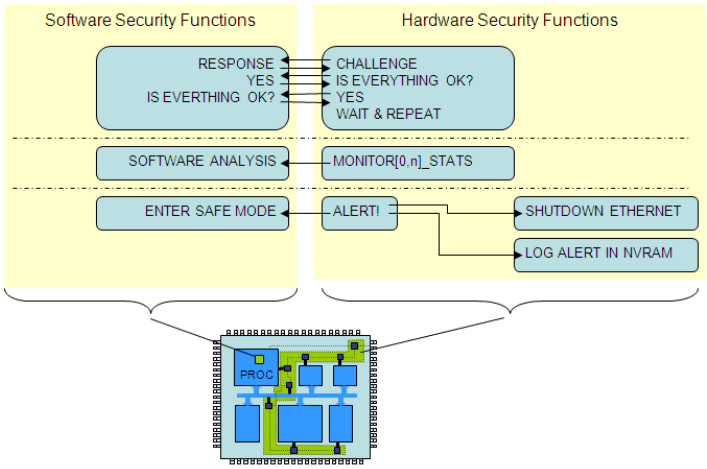

Figure 2: Hardware ⇔ Software Interaction

There are many advantages of using multiple and distributed programmable monitors. With multiple programmable monitors instantiated within different clock domains, power domains,

and functional domains, a full *system* view can be realized. Moreover, the monitors can be tied together with cross-triggering signals so that more elaborate intra-domain and inter-domain conditions can be analyzed. This provides similar benefits to the hardware ⇔ software interactions described above. Sprinkling multiple programmable monitors throughout the design also provides redundancy. Monitors can keep an eye on each other; when an attacker attempts to manipulate the power, clocks, or functionality in one subsystem, the monitors in the other subsystem will be alerted.

As with embedded processors, the value of programmability cannot be underestimated. The fact that the programmable monitors can be repurposed at any point in time is crucial. Monitors can be programmed *in-system* to perform different functions over time. By time-slicing functionality, a wider range of misbehaviors can be detected with the same resource. To the attacker, this creates the appearance of random countermeasures and ultimately makes his efforts to tamper or reverse-engineer the system much more difficult.

Obvious concerns are whether the programmable monitors are more vulnerable and whether they in fact provide additional portals of attack. The simple answer is no. There are multiple security features within the SbV system. The embedded communication channel is secure and the programming files are encrypted, making it virtually impossible for an attacker to make undetected modifications to a programmable monitor. Cross-triggering between monitors and the handshakes with software provide a reliable and redundant "neighborhood watch" and early warning system. Additionally, the fact that the programmable fabric is inserted with automated tools ensures that the system is correct by construction, reducing the possibility that an implementation flaw will enable a breach. Ultimately, the inclusion of this programmable fabric will greatly increase the overall system security, allowing the protection of intellectual property while at the same time protecting the end systems and the data stored within.

--

The use of programmable logic extends beyond anti-tamper and countermeasure applications. SbV is developing new applications with programmable fabric to address anti-counterfeit and feature activation control – two key components required to secure supply chains and protect critical assets.

The anti-counterfeit and feature activation solutions are closely related. The anti-counterfeit solution uses a combination of programmable logic and one-time-programmable memory to store unique encrypted codes within a device. Devices are programmed and subsequently authorized through a secure JTAG interface using SbV's software security application. SbV is developing two schemes for generating unique ID codes for each device. One relies on a central off-chip ID generation scheme, while the other uses GPS technology developed in partnership with Professor Per Enge and his colleagues Dr. Sherman Lo and Dr. David De Lorenzo of Stanford's GPS Research Laboratory in the University's Department of Aeronautics & Astronautics. Additional information is available under a non-disclosure agreement.

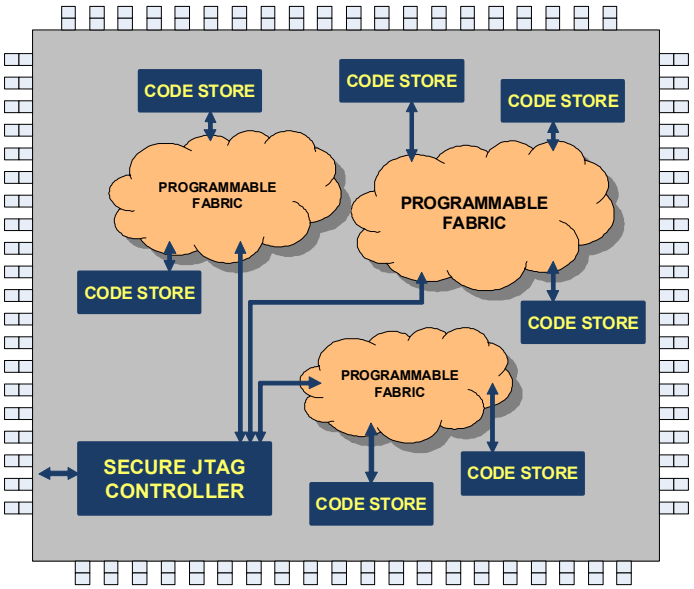

Figure 3 : ID code store

The combined use of distributed ID code storage and distributed programmable logic structures increases code security, as one must compromise the encryption key, the programmable logic programming protocol, and the programmable bitfile(s). In addition, not only will *each* device store a unique encrypted ID, but *each* ID is written and retrieved using a different programming bitfile, meaning the bits of the code will be scrambled in different locations on each device. The distributed programmable logic structures also provide a measure of obfuscation to thwart efforts to uncover the codes by de-capping the device.

Feature activation also uses a combination of non-volatile or one-time-programmable memory in conjunction with programmable logic wrappers. These wrappers are inserted on key control signals such as resets, mode controls, or power controls. The wrappers can be controlled by software, through a secure factory programming channel, or both.

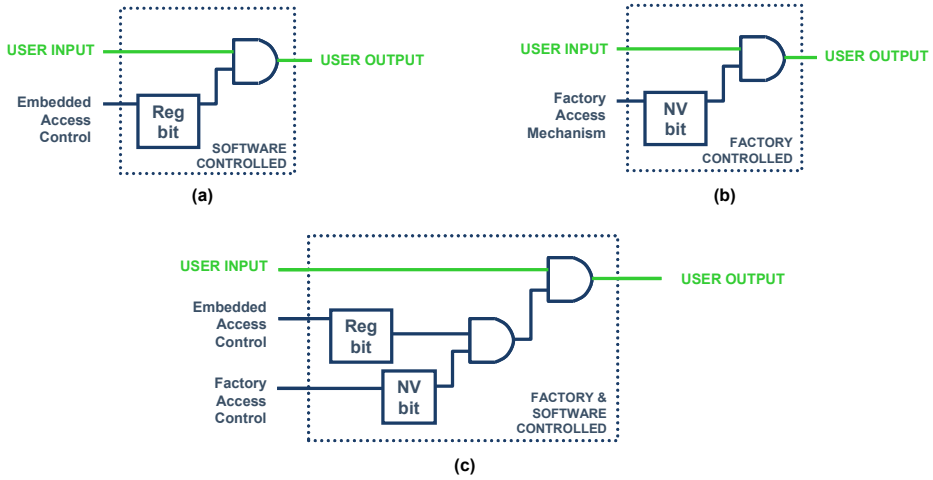

Figure 4 : Feature Activation Wrappers – Basic Wrapper Concept

The wrappers are inserted using automated tools during the pre-silicon hardware design phase. The choice of wrapper type is dependent on the security, configuration and authentication requirements of a device or system. For example, features that need to be enabled or disabled in the field need software controlled wrappers, whereas features that must be enabled in the factory need factory control wrappers. The combination of factory and software controlled wrapper as shown in Figure 5 (c) enables additional flexibility. While not shown in Figure 5, wrappers can be controlled by previously described programmable logic monitors. For example, a wrapper may be enabled only if select monitoring functions are enabled. Or conversely, a wrapper may be disabled as a result of tampering activity detected in a monitor.

The deactivation of a previously activated feature (or even a feature not yet activated) can be volatile or non-volatile. If certain tampering or unauthorized activities are detected, features can be permanently disabled. Permanent deactivation, however, is only possible if one-time-programmable storage is designed into the wrapper.

Both the external and internal programming interfaces are secure, and all program bit files are stored in encrypted form.

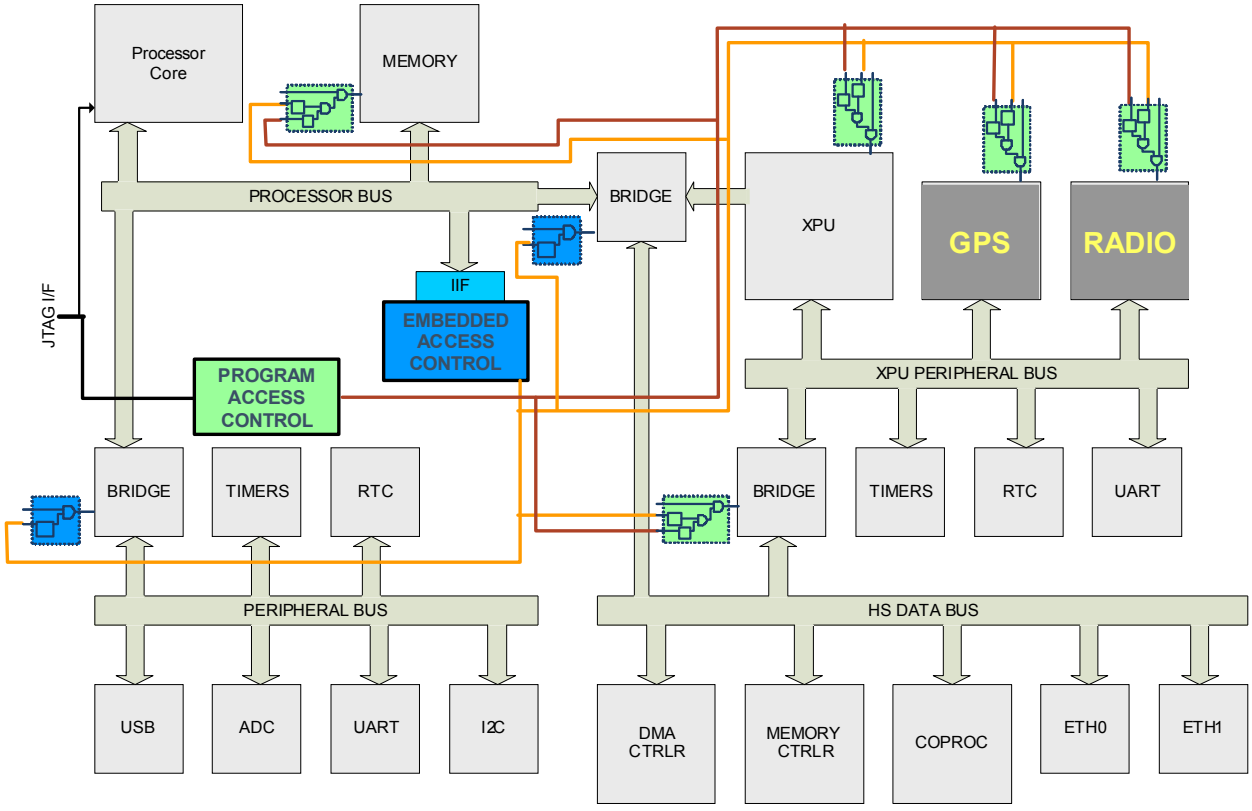

Figure 5 : System with Feature Activation Wrappers

--

Key Benefits of SbV Technology

- Protect your investment
  - SbV's novel programmable logic structures are used to protect the system and provide assurance that any new and unexpected threats or security flaws can be mitigated through firmware or software upgrade.
- Protect your customers
  - Suppliers of consumer products and semiconductor manufacturers can reduce customers' exposure to security threats by providing assurance that their devices and critical data are transferred through or stored in the most secure devices.
- Low-cost / low-risk implementation
  - SbV's silicon-proven IP and powerful automated insertion tools allow innovative and robust security schemes to be constructed without significant impact to schedules or budgets.
- Designed-in quality
  - Automated insertion and reuse allow corporations to leverage SbV's technology with the confidence that complexity does not increase design risk or device vulnerability.

About Sawblade Ventures

Sawblade Ventures, LLC. (www.sawbladeventures.com) is leveraging its silicon-proven core technology in System and Device Security solutions to address anti-tamper/reverse engineering, countermeasure, feature activation, and anti-counterfeit. For more information, send email to info@sawbladeventures.com .