consumption of the platform and concentrating on trace sections carrying the most information about the internal execution status; by improving the ability of PFP to detect deviations from authorized execution in commercial embedded platforms.

An aspect of the invention is a method for performing real-time integrity assessment of execution of a routine in a computer processing platform. This is accomplished by monitoring execution of the routine by tracing power consumption of a processor, by sampling the processor during execution of the routine. A platform characterization technique is employed that detects sections of the traces, that is, those sections that display the largest dependence on state transitions in the processor. These sections are used to select features carrying the most information. This platform characterization applies to the platform and can be used for all routines run on the platform. The next step is to obtain, from a characterization of selected features of the routine, as contained in the sections identified in the platform characterization, a set of trusted power fingerprints of the routine. Then there is established a threshold for a specific false alarm rate based on the probability distribution of distance from a signature comprised of the trusted fingerprints. A library of the trusted fingerprints is then compared to features extracted from traces from the execution of untrusted code, and there is then determined a distance between the fingerprints in the library and the features extracted from execution of the untrusted code. An exception is reported if the distance exceeds the threshold.

[008a] An aspect of the invention is a system for performing real-time integrity assessment of execution of a routine in a computer processing platform, comprising: means for monitoring execution of the routine by tracing power consumption of a processor by sampling during execution of the routine; means for using a platform characterization technique that further comprises means for detecting sections of the traces that display the largest dependence on state transitions in the processor; means for using said sections to select features carrying the most information; means for obtaining from a characterization of the selected features contained in said sections a set of trusted power fingerprints of the routine; means for establishing a threshold for a specific false alarm rate based on the probability distribution of distance from a signature comprised of said trusted fingerprints; means for comparing a library of said trusted fingerprints to features extracted from traces

from the execution of untrusted code means for determining a distance between said fingerprints and the extracted features; and means for reporting an exception if the distance exceeds the threshold.

[008b] An aspect of the invention is a method for detecting deviations from authorized execution of software in a digital processor, comprising: observing power consumption of the processor during execution of at least one routine of the software in a known setting; determining a sequence of bit transitions characterizing the power consumption of said at least one routine; and using the power consumption characterization as a fingerprint for comparison against observed execution of the software to determine deviation.

[009] Various procedures for improving the operation, effectiveness, usability, and performance of integrity assessment and intrusion detection systems based on power fingerprinting (PFP) are described. The different procedures include:

- Embedding module identification information into synchronization signaling
- Improved PFP monitoring by combining signals from different board elements
- Using malware signatures to enhance PFP performance, generalizing on existing battery monitoring technology.
- Automatic characterization and signature extraction