

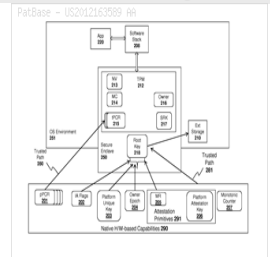
1) Family number: 51343900 (US2012163589 AA)

SYSTEM AND METHOD FOR IMPLEMENTING A TRUSTED DYNAMIC LAUNCH AND TRUSTED PLATFORM MODULE (TPM) USING SECURE ENCLAVES

Abstract: Source: US2012163589 AA An apparatus and method are described for implementing a trusted dynamic launch and trusted platform module (TPM) using a secure enclave. For example, a computer-implemented method according to one embodiment of the invention comprises: initializing a secure enclave in response to a first command, the secure enclave comprising a trusted software execution environment which prevents software executing outside the enclave from having access to software and data inside the enclave; and executing a trusted platform module (TPM) from within the secure enclave, the trusted platform module securely reading data from a set of platform control registers (PCR) in a processor or chipset component into a memory region allocated to the secure enclave.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20120628

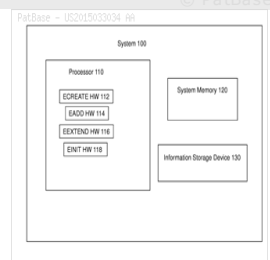


2) Family number: 58396684 (US2015033034 AA)

MEASURING A SECURE ENCLAVE

Abstract: Source: US2015033034 AA Embodiments of an invention for measuring a secure enclave are disclosed. In one embodiment, a processor includes an instruction unit and an execution unit. The instruction unit is to receive a first, a second, and a third instruction. The execution unit is to execute the first, the second, and the third instruction. Execution of the first instruction includes initializing a measurement field in a control structure of a secure enclave with an initial value. Execution of the second instruction includes adding a region to the secure enclave. Execution of the third instruction includes measuring a subregion of the region.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20150129

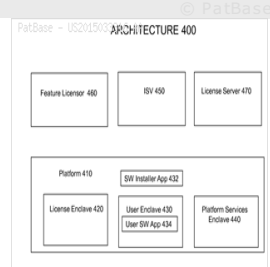
3) Family number: 58397147 (US2015033316 AA)

FEATURE LICENSING IN A SECURE PROCESSING ENVIRONMENT

Abstract: Source: US2015033316 AA Embodiments of an invention for feature licensing in a secure processing environment are disclosed. In one embodiment, a processor includes an instruction unit and an execution unit. The instruction unit is to receive an instruction to initialize a secure enclave. The execution unit is to execute the instruction. Execution of the instruction includes determining whether a requested feature is licensed for use in the secure enclave.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20150129

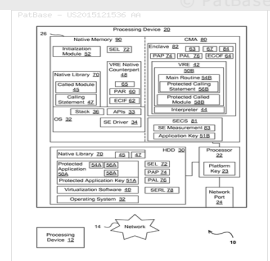


4) Family number: 59087676 (US2015121536 AA)

METHODS AND APPARATUS FOR PROTECTING SOFTWARE FROM UNAUTHORIZED COPYING

Abstract: Source: US2015/011536 AA A processing device provides a method for protecting a program from unauthorized copying. The processing device may include an encrypted version of the program. According to one example method, the processing device creates a secure enclave, and in response to a request to execute the encrypted program, the processing device automatically generates a decrypted version of the program in the secure enclave by decrypting the encrypted program in the secure enclave. After automatically generating the decrypted version of the program in the secure enclave, the processing device may automatically execute the decrypted version of the program in the secure enclave. Other embodiments are described and claimed.

Probable Assignee: INTEL CORP

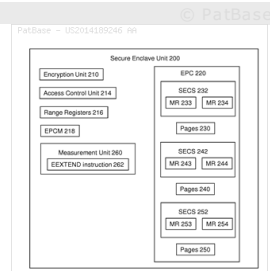
Earliest Publication Date: 20150430

5) Family number: 56830195 (US2014189246 AA)

MEASURING APPLICATIONS LOADED IN SECURE ENCLAVES AT RUNTIME

Abstract: Source: US2014189246 AA Embodiments of an invention for measuring applications loaded in secure enclaves at runtime are disclosed. In one embodiment, a processor includes an instruction unit and an execution unit. The instruction unit is to receive an instruction to extend a first measurement of a secure enclave with a second measurement. The execution unit is to execute the instruction after initialization of the secure enclave.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20140703

```

graph TD
    subgraph System_100 [System 100]
        subgraph Processor_110 [Processor 110]
            I11[Instruction Unit 111]
            E12[Execution Unit 112]
            P13[Processing Storage 113]
            I14[Interface Unit 114]
            P15[Processor Control Unit 115]
            C16[Cache Memory 116]
            IO17[I/O Unit 117]
        end
        subgraph System_Memory_120 [System Memory 120]
            S121[Secure Memory 121]
            D124[DRAM 124]
        end
        subgraph Secure_Units [Secure Encipher Unit 123, Encryption Unit 122, Firmware 124, Access Control Unit 125]
            S123[Secure Encipher Unit 123]
            E122[Encryption Unit 122]
            F124[Firmware 124]
            A125[Access Control Unit 125]
        end
    end
    Processor_110 --- System_Memory_120
    Processor_110 --- Secure_Units
    Secure_Units --- ISD140[Information Storage Device 140]

```

PatBase - US2015222633 A1

300

```

graph LR
    subgraph Client_101 [Client 101]
        subgraph Device_Platform_104 [Device Platform 104]
            subgraph Processor_105 [Processor 105]
                AE_108 [AE 108]
            end
            Memory_106 [Memory 106]
            IO_107 [IO 107]
        end
        subgraph AE_108 [AE 108]
            PEM_109 [PEM 109]
            Policy_110 [Policy 110]
        end
        subgraph SIPE_111a [SIPE 111, DRAM 112a]
            DRAM_112a [DRAM 112a]
        end
        subgraph SIPE_111b [SIPE 111, DRAM 112b]
            DRAM_112b [DRAM 112b]
        end
    end
    Processor_105 --- AE_108
    AE_108 --- SIPE_111a
    AE_108 --- SIPE_111b
    SIPE_111a --- Sensor_301a [Sensor 301]
    SIPE_111b --- Sensor_301b [Sensor 301]
    Sensor_301a --- Sensor_Data_302a [Sensor Data 302a]
    Sensor_301b --- Sensor_Data_302b [Sensor Data 302b]

```

PatBase - US2014157404 AA

PatBase - US2014157404 AA

[illegible]

100% DatBase - US2016171248 AA

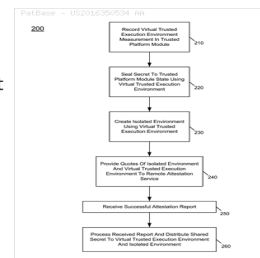
Figure 1 illustrates the Operating System architecture. It shows a stack of 'Other Apps' (118, 119, 120) at the top, followed by an 'Application' (112) and a 'Trusted Agent TAE' (110). The 'Trusted Agent TAE' is connected to a 'Trusted Manager TAE' (108) via a bidirectional link (132). The 'Trusted Manager TAE' is connected to a 'CloudService Service' (124) via a bidirectional link (134). The entire system is labeled 'Operating System' at the bottom.

SYSTEM, APPARATUS AND METHOD FOR CONTROLLING MULTIPLE TRUSTED EXECUTION ENVIRONMENTS IN A SYSTEM

Abstract: Source: US2016350534 AA In an embodiment, a system is adapted to: record at least one measurement of a virtual trusted execution environment in a storage of the system and generate a secret sealed to a state of this measurement; create, using the virtual trusted execution environment, an isolated environment including a secure enclave and an application, the virtual trusted execution environment to protect the isolated environment; receive, in the application, a first measurement quote associated with the virtual trusted execution environment and a second measurement quote associated with the secure enclave; and communicate quote information regarding the first and second measurement quotes to a remote attestation service to enable the remote attestation service to verify the virtual trusted execution environment and the secure enclave, and responsive to the verification the secret is to be provided to the virtual trusted execution environment and the isolated environment. Other embodiments are described and claimed.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20161201



12) Family number: 59608189 (US2015347768 AA)

POLICY-BASED TRUSTED INSPECTION OF RIGHTS MANAGED CONTENT

Abstract: Source: US2015347768 AA An embodiment includes a method executed by at least one processor comprising: initializing first and second secure enclaves each comprising a trusted software execution environment that prevents software executing outside the first and second secure enclaves from having access to software and data inside the first and second secure enclaves; the first secure enclave (a)(i) inspecting a policy, (a)(ii) authenticating the second secure enclave in response to inspecting the policy; and (a)(iii) communicating encrypted content to the second secure enclave in response to authenticating the second secure enclave; and the second secure enclave (b)(i) decrypting the encrypted content to produce decrypted content, and (b)(ii) inspecting the decrypted content. Other embodiments are described herein.

Probable Assignee: INTEL CORP

Earliest Publication Date: 20150625

