# XX TCG MOR Test

### XX.1TCG MOR Test

Reference Document:

*TCG PC Platform Reset Attack Mitigation Specification*,v1.10 Revision 17, January 21, 2019, Chapter 4.

These tests support platform firmware that implements the MemoryOverwriteRequestControl and MemoryOverwriteRequestControlLock UEFI variables in accordance with TCG PC Platform Reset Attack Mitigation Specification, v1.10.

### XX.1.1 MemoryOverwriteRequestControl Platform Reset Check

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
|  |  | Verify MemoryOverwriteRequestControl is created by platform firmware as specified in the TCG specification. | 1. Reboot the system.  2. Verify GetVariable() returns MemoryOverwriteRequestControl with correct attributes = (NV+RT+BS) and correct DataSize = 1.  If MemoryOverwriteRequestControl does not exist, the test should exit with an exit code that notifies user TCG MOR is not enabled on platform.  If MemoryOverwriteRequestControl exists with the incorrect attributes or DataSize, the test should report an error. |
|  |  | Set the MemoryOverwriteAction\_BitValue within MemoryOverwriteRequestControl.  Verify that on System reset, the MemoryOverwriteAction\_BitValue is cleared. | 1. Invoke SetVariable() with valid GUID, variable name, attributes, and DataSize and Set MemoryOverwriteAction\_BitValue Bit 0.  2. Reboot System.  3. Invoke GetVariable() with valid GUID, variable name, attributes, and DataSize.  4. Verify MemoryOverwriteAction\_BitValue Bit 0 is Cleared. |
|  |  | Verify MemoryOverwriteRequestControlLock is created by platform firmware as specified in the TCG specification. | 2. Verify GetVariable() returns MemoryOverwriteRequestControlLock with correct attributes = (NV+RT+BS), correct DataSize = 1, and correct Data = 0 to indicate unlocked.  If MemoryOverwriteRequestControlLock does not exist, the test should exit with an exit code that notifies user TCG MORlock is not enabled on platform.  If MemoryOverwriteRequestControlLock exists with the incorrect attributes or DataSize, or the Data != 0 indicating the variable is not unlocked, the test should report an error. |
| N/A | N/A | Set the MemoryOverwriteAction\_BitValue within MemoryOverwriteRequestControl.  Verify that on System reset, the Platform’s memory has been cleared. | Based on our analysis so far, this might not be possible to do reliably in a system agnostic manner. |

### XX.1.2 MemoryOverwriteRequestControl.SetVariable()

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
|  |  | MemoryOverwriteRequestControl.SetVariable() returns EFI\_INVALID\_PARAMETER by passing in all valid parameters aside from an incorrect DataSize = 0.  The state of MemoryOverwriteRequestControl shall not change. | 1. Invoke GetVariable()with valid GUID, variable name, attributes and DataSize. Save the current value for comparison.  2. Invoke SetVariable() with valid GUID, variable name, and attributes. DataSize set to 0 and Data is != saved value from the previous step.  a. Verify SetVariable() returns EFI\_INVALID\_PARAMETER.  b. Verify that MemoryOverwrit-eRequestControl GetVariable() returns a Data value == initial saved value of MemoryOverwriteRequestControl. |
|  |  | MemoryOverwriteRequestControl.SetVariable() returns EFI\_INVALID\_PARAMETER by passing in all valid parameters aside from incorrect attributes.  The state of MemoryOverwriteRequestControl shall not change. | 1. Invoke GetVariable()with valid GUID, variable name, attributes and DataSize. Save the current value for comparison.  2. Invoke SetVariable() with valid GUID, variable name, and DataSize. Pass an attributes value != (NV+RT+BS) and Data != saved value from the previous step.  a. Verify SetVariable() returns EFI\_INVALID\_PARAMETER.  b. Verify that MemoryOverwrit-eRequestControl GetVariable() returns a Data value == initial saved value of MemoryOverwriteRequestControl. |

### XX.1.3 MemoryOverwriteRequestControlLock.SetVariable()

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
|  |  | MemoryOverwriteRequestControlLock.SetVariable() passing valid parameters excluding Attributes == 0 must return EFI\_WRITE\_PROTECTED.  The state of MemoryOverwriteRequestControlLock shall not change. | 1. Reboot the system to ensure MemoryOverwriteRequestControlLock is unlocked.  2. Invoke SetVariable() with valid GUID, variable name, Data, and DataSize. Pass an attributes value == 0.   1. Verify SetVariable() returns EFI\_WRITE\_PROTECTED. 2. Verify that MemoryOverwriteRequestControlLock GetVariable() returns a Data Value == 0. |
|  |  | MemoryOverwriteRequestControlLock.SetVariable() passing valid parameters excluding DataSize == 0 must return EFI\_WRITE\_PROTECTED.  The state of MemoryOverwriteRequestControlLock shall not change. | Invoke SetVariable() with valid GUID, variable name, Data, and Attributes. Pass DataSize== 0.   1. Verify SetVariable() returns EFI\_WRITE\_PROTECTED. 2. Verify that MemoryOverwriteRequestControlLock GetVariable() returns a Data Value == 0. |
|  |  | MemoryOverwriteRequestControlLock.SetVariable() passing valid parameters excluding Data == NULL must return EFI\_WRITE\_PROTECTED.  The state of MemoryOverwriteRequestControlLock shall not change. | Invoke SetVariable() with valid GUID, variable name, Attributes, and DataSize. Pass Data == NULL.   1. Verify SetVariable() returns EFI\_WRITE\_PROTECTED. 2. Verify that MemoryOverwriteRequestControlLock GetVariable() returns a Data Value == 0. |
|  |  | MemoryOverwriteRequestControlLock.SetVariable() passing valid parameters and Attributes != (NV+BS+RT) must return EFI\_INVALID\_PARAMETER.  The state of MemoryOverwriteRequestControlLock shall not change. | Invoke SetVariable() with valid GUID, variable name, Data, and DataSize. Set Attributes != (NV+BS+RT).   1. Verify SetVariable() returns EFI\_INVALID\_PARAMETER. 2. Verify that MemoryOverwriteRequestControlLock GetVariable() returns a Data Value == 0. |
|  |  | MemoryOverwriteRequestControlLock.SetVariable() passing valid parameters excluding (DataSize != 1 && DataSize != 8) must return EFI\_INVALID\_PARAMETER.  The state of MemoryOverwriteRequestControlLock shall not change. | Invoke SetVariable() with valid GUID, variable name, Data, and Attributes. Set DataSize != 1 && DataSize != 8.   1. Verify SetVariable() returns EFI\_INVALID\_PARAMETER. 2. Verify that MemoryOverwriteRequestControlLock GetVariable() returns a Data Value == 0. |

### XX.1.4 MemoryOverwriteRequestControlLock Unlocked state

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
|  |  | Setting MemoryOverwriteRequestControlLock to Unlocked State when already Unlocked should using SetVariable should return EFI\_SUCCESS and a data value of 0(Unchanged). | 1. Reboot System to make firmware initialize MemoryOverwriteRequestControlLock to Unlocked.  2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize = 1, and Data = 0.   1. Verify Lock.SetVariable() returns EFI\_SUCCESS.   3. Invoke GetVariable() with valid GUID, variable name, attributes, DataSize.   1. Verify that the output value is 0. |
|  |  | Setting MemoryOverwriteRequestControlLock with an invalid first byte for Data when in Unlocked State should return EFI\_INVALID\_PARAMETER. | Invoke SetVariable() with valid GUID, variable name, attributes, DataSize = 1, Data first byte != 0 && Data first byte != 1.   1. Verify SetVariable() returns EFI\_INVALID\_PARAMETER |

### XX.1.5 MemoryOverwriteRequestControlLock Locked w/o key state

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
|  |  | Changing MemoryOverwritRequestControlLock to Locked state without key Should return EFI\_SUCCESS when MemoryOverwriteRequestControlLock is currently unlocked. | 1. Reboot System to make firmware initialize MemoryOverwriteRequestControlLock to Unlocked.  2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 1.   1. Verify SetVariable() returns EFI\_SUCCESS. 2. Verify GetVariable() returns Data value of 1. |
|  |  | Changing MemoryOverwriteRequestControlLock to Unlocked state Should return  EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock is currently Locked without key. | 1. Verify MemoryOverwriteRequestControlLock is currently locked without key.   1. Verify GetVariable() returns Data value of 1.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 0.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value of 1. |
|  |  | Changing MemoryOverwriteRequestControlLock to Locked without key state Should return EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock is currently Locked without key. | 1. Verify MemoryOverwriteRequestControlLock is currently locked without key.   1. Verify GetVariable() returns Data value of 1.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 1.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value 1. |
|  |  | Changing MemoryOverwriteRequestControlLock to Locked state with key  Should return EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock was already Locked without key. | 1. Verify MemoryOverwriteRequestControlLock is currently locked without key.   1. Verify GetVariable() returns Data value of 1.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 8-byte user generated key.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value 1. |

### XX.1.6 MemoryOverwriteRequestControlLock Locked state with key

|  |  |  |  |
| --- | --- | --- | --- |
| Number | GUID | Assertion | Test Description |
| x.x |  | Changing MemoryOverwriteRequestControlLock to Locked state with a key  must return EFI\_SUCCESS when MemoryOverwriteRequestControlLock is currently unlocked.    MemoryOverwriteRequestControlLock must be locked with key. | 1. Reboot System to make firmware initialize MemoryOverwriteRequestControlLock to Unlocked.  2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 8-byte user generated key.   1. Verify SetVariable() returns EFI\_SUCCESS. 2. Verify GetVariable() returns Data value 2. |
|  |  | Changing MemoryOverwriteRequestControlLock to Unlocked state with the 8 byte key used in the previous SetVariable() Lock with key action  must return EFI\_SUCCESS when MemoryOverwriteRequestControlLock is currently Locked with key.    MemoryOverwriteRequestControlLock must be unlocked. | 1. Verify MemoryOverwriteRequestControlLock is currently locked with 8-byte user generated key.   1. Verify GetVariable() returns Data value 2.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 8-byte user generated key that was used to set the lock in test number x.x.   1. Verify SetVariable() returns EFI\_SUCCESS. 2. Verify GetVariable() returns Data value 0. |
|  |  | Changing MemoryOverwriteRequestControlLock to Unlocked state with an invalid DataSize must return EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock is currently Locked with key.    MemoryOverwriteRequestControlLock must not change. | 1. Verify MemoryOverwriteRequestControlLock is currently locked with 8-byte user generated key.   1. Verify GetVariable() returns Data value 2.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, and DataSize != 8.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value 2. |
|  |  | Changing MemoryOverwriteRequestControlLock to Locked without key state must return EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock is currently Locked with key.    MemoryOverwriteRequestControlLock must not change. | 1. Verify MemoryOverwriteRequestControlLock is currently locked with 8-byte user generated key.   1. Verify GetVariable() returns Data value 2.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 1.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value 2. |
|  |  | Changing MemoryOverwriteRequestControlLock to Unlocked state with an 8 byte value that is not equal to the 8-byte key used in the previous SetVariable() Lock with key action  must return EFI\_ACCESS\_DENIED when MemoryOverwriteRequestControlLock is currently Locked with key. | 1. Verify MemoryOverwriteRequestControlLock is currently locked with 8-byte user generated key.   1. Verify GetVariable() returns Data value 2.   2. Invoke SetVariable() with Valid GUID, variable name, attributes, DataSize, and Data Input = 8 byte value != 8-byte user generated key from test number x.x.   1. Verify SetVariable() returns EFI\_ACCESS\_DENIED. 2. Verify GetVariable() returns Data value 1. |