SAND2017-7573C

The Center for Cyber Defenders

Expanding computer security knowledge

STM-based Introspection

A Platform for Analysis of Low-level Security Solutions

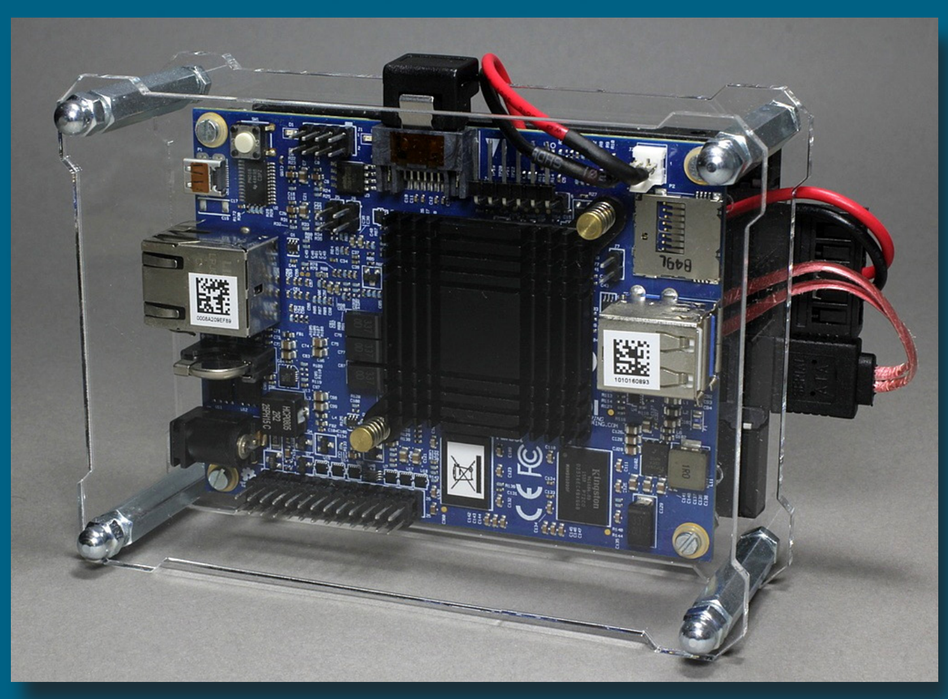
Min Je Jung, Georgia Institute of Technology
Tiemoko Ballo, Carnegie Mellon University

Project Mentors: Rob Bell, Org.5834 and Russell Graves, Org. 6612

Problem Statement:

System Management Mode (SMM) is the most privileged mode of execution on x86(64) architecture. SMM code can bypass and subvert hypervisor based security solutions. In an effort to prevent SMM exploitation, Intel introduced the STM (SMI Transfer Monitor) – an SMM hypervisor.

Though the first STM implementation was introduced in August 2015, little documentation exists and the security implications are not yet well understood. We seek to investigate using STM technology to debug and analyze low-level security solutions.



The MinnowBoard Turbot
(opendisplaycase.com)

Objectives and Approach:

- Build upon Intel's base hypervisor
- Develop and test on open-source hardware (MinnowBoard Turbot)
- Characterize STM capability
- Invent novel and reliable ways to transfer control to the STM at chosen points in time
- Implement introspection and debugging functionality within the STM
- Implement a remote command interface for the STM over high speed serial
- Use the introspection STM to evaluate OS use of Intel's HW security features

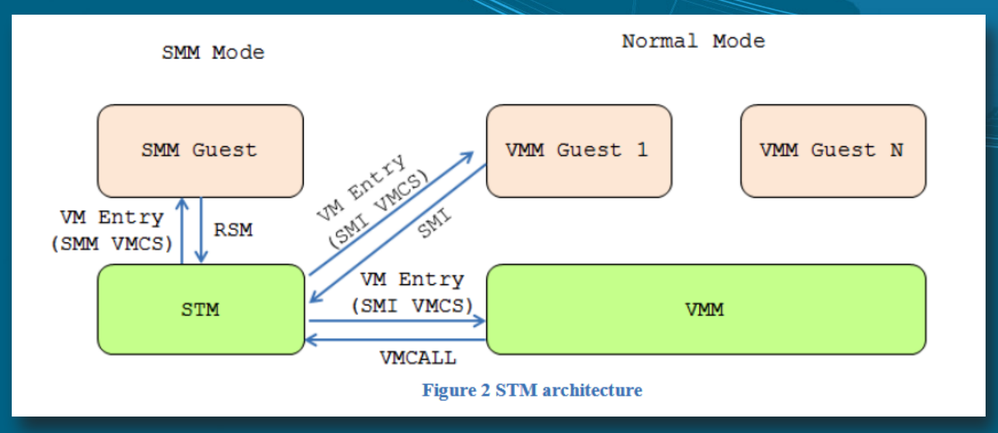


Figure 2 STM architecture

Execution Modes for Virtualized x86
(Jiewen Yao, Vincent J. Zimmer, "A Tour Beyond BIOS *Launching a STM to Monitor SMM in EFI Developer Kit II", August 2015)*

Results:

- Implemented VMM handlers for RDTSCP and RDTSC instruction support, giving the hypervisor control over timing information presented to guest VMs
- Integrated an open-source disassembler (diStorm3) that runs in the STM environment and supports abstract representations of instructions/operands
- Extended introspection STM functionally with a new command to disassemble user-specified regions of memory and output the results over high speed serial
- Will investigate options for systematically tracking of control flow and code coverage from the STM

```
(STM-0)00000001 (01) ee                     OUT DX, AL
(STM-0)00000002 (02) 2ecf                   IRET
(STM-0)00000004 (03) 0f53e3                 RCPPS XMM4, XMM3
(STM-0)00000007 (03) 11406d                 ADC [RAX+0x6d], EAX
(STM-0)0000000a (01) c4                     DB 0xc4
(STM-0)0000000b (01) 8e                     DB 0x8e
(STM-0)0000000c (01) fa                     CLI
(STM-0)0000000d (02) 7399                   JAE 0xfffffffffffffa8
(STM-0)0000000f (02) 0132                   ADD [RDX], ESI
(STM-0)00000011 (01) 8e                     DB 0x8e
(STM-0)00000012 (02) 7dff                   JGE 0x13
(STM-0)00000014 (08) 264bf71d86f02740       NEG QWORD [RIP+0x4027f086]
(STM-0)0000001c (07) 8b9421f2c6ac07         MOV EDX, [RCX+0x7acc6f2]
(STM-0)00000023 (01) ee                     OUT DX, AL
(STM-0)00000024 (01) 9b                     WAIT
(STM-0)00000025 (06) 43a9195efe4b           TEST EAX, 0x4bfe5e19
(STM-0)0000002b (01) c7                     DB 0xc7
(STM-0)0000002c (05) 3dd7fad31d             CMP EAX, 0x1dd3fad7
(STM-0)00000031 (07) 0feabf6d6bd28d         PMINSW MM7, [RDI-0x722d9493]
(STM-0)00000038 (02) da3e                   FIDIVR DWORD [RSI]
(STM-0)0000003a (02) 0927                   OR [RDI], ESP
(STM-0)0000003c (02) 1ca7                   SBB AL, 0xa7
(STM-0)0000003e (01) ea                     DB 0xea
(STM-0)0000003f (02) eb03                   JMP 0x44
(STM-0)00000041 (05) bc65e6aac7             MOV ESP, 0xc7aae665
(STM-0)00000046 (02) b15b0)00000048 (01) c5                 DB 0xc5
(STM-0)00000049 (05) bf86e75bc7             MOV EDI, 0xc75be786
(STM-0)0000004e (01) c9                     LEAVE
(STM-0)0000004f (01) 5b                     POP RBX
(STM-0)00000050 (02) 84f4                   TEST AH, DH
(STM-0)00000052 (04) 26c28bd5               RET 0xd58b
```

High Speed Serial Disassembly Output from the STM

Impact and Benefits:

- Gain and document knowledge of new Intel security mechanisms and their implementation in modern operating systems
- Create a security research platform that provides unparalleled visibility into low-level Intel security mechanisms

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology and Engineering Solutions of Sandia, LLC., a wholly owned subsidiary of Honeywell International, Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525. SAND2017-XXXXC.