TrustLogin: Securing Password-Login On Commodity Operating Systems

Fengwei Zhang [1] Kevin Leach [2] Haining Wang [3]
Angelos Stavrou [1]

[1]Wayne State University

[2]University of Virginia

[3]University of Delaware

November 16, 2015

Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

Motivation

Keylogger examples

- Keylogger malware found on UC Irvine health center in May 2014, and about two thousand students were impacted [1]
- Attackers have stolen credit card information for customers who shopped at 63 Barnes & Noble stores using keyloggers [2]
- A case study has shown that 10,775 unique bank account credentials were stolen by keyloggers in a seven-month period [3]

Protecting login credentials is a critical part of daily life

Motivation

- OS as a trusted computing base, which has a large amount of source code
  - Linux kernel has 17M lines of code
  - CVE shows 240 vulnerabilities for the Linux kernel
- An attacker can compromise the OS and install a stealthy keylogger
  - Banking, SSH login passwords

Our Approach

We present TrustLogin, a framework to securely perform login operations using System Management Mode (SMM)

- Prevent rootkits and stealthy keyloggers without trusting the OS
- Does not change any software on the client and server sides
- Transparent to users and applications

Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

Background: System Management Mode

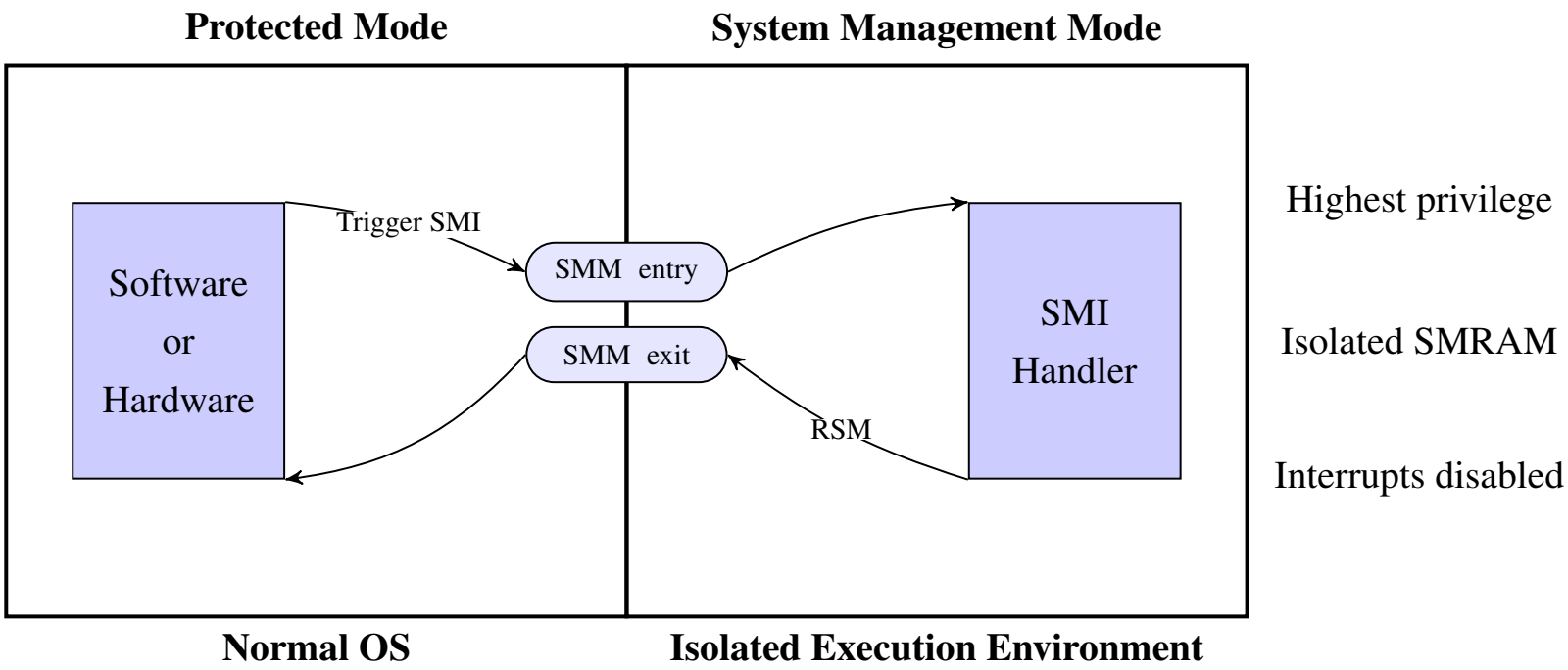
System Management Mode (SMM) is special CPU mode existing in x86 architecture, and it can be used as a hardware isolated execution environment.

- Originally designed for implementing system functions (e.g., power management)
- Isolated System Management RAM (SMRAM) that is inaccessible from OS
- Only way to enter SMM is to trigger a System Management Interrupt (SMI)
- Executing `RSM` instruction to resume OS (Protected Mode)

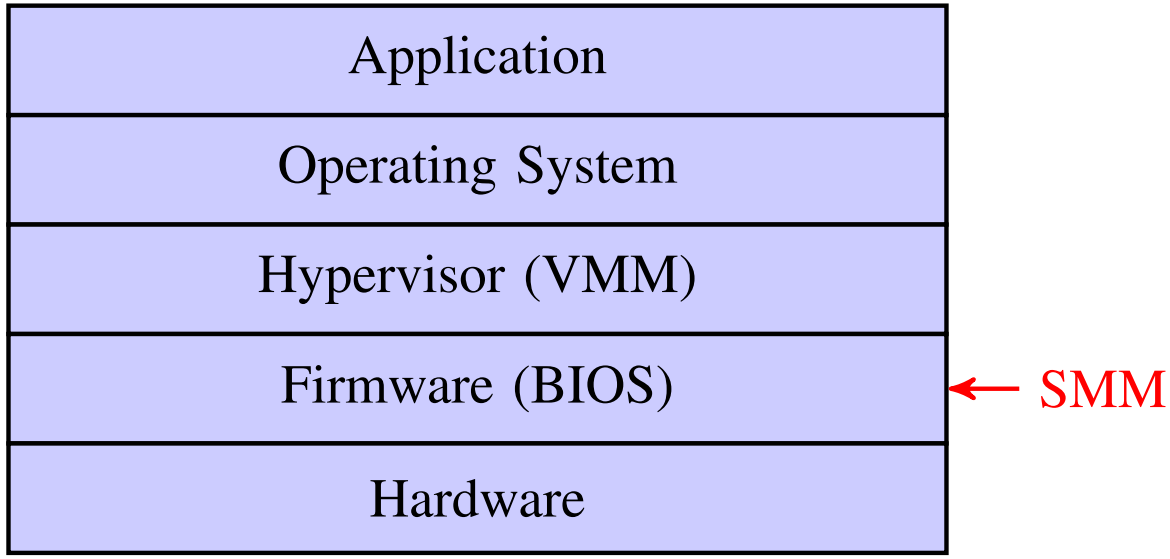
Background: System Management Mode

Approaches for Triggering a System Management Interrupt (SMI)

- Software-based: Write to an I/O port specified by Southbridge datasheet (e.g., 0x2B for Intel)
- Hardware-based: Network card, keyboard, hardware timers



Background: Software Layers



Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

System Framework

- SMM provides a secure world; we move the security sensitive operations into it.

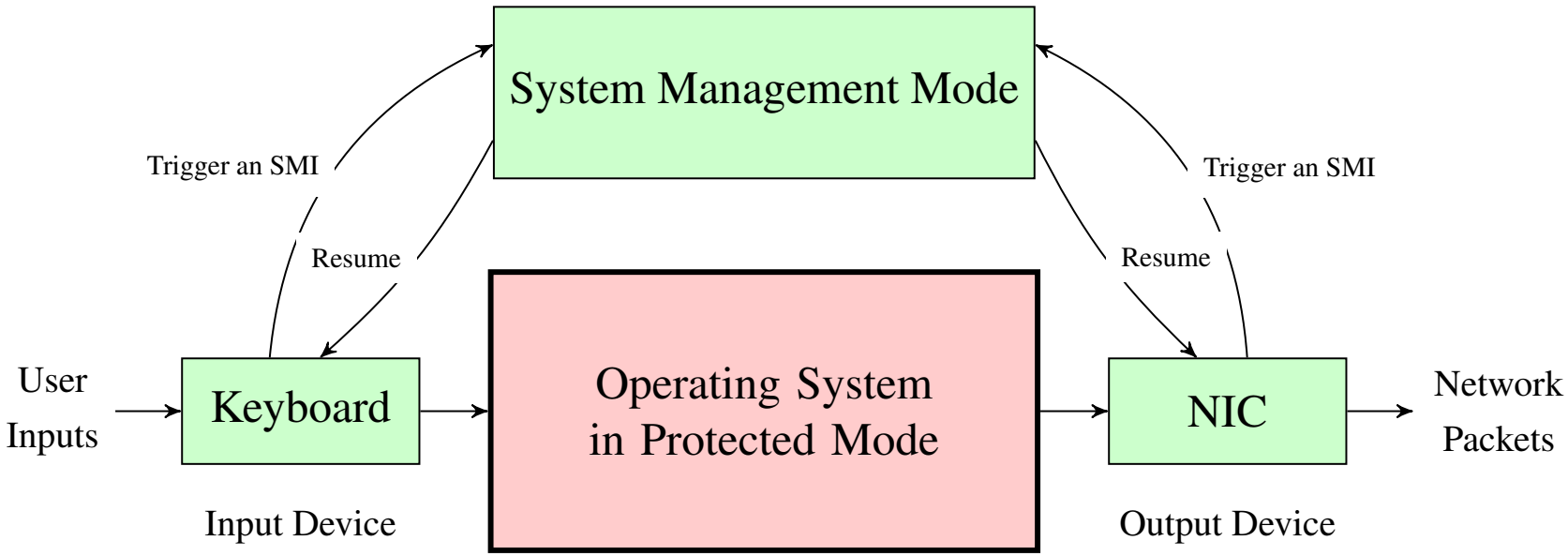


Figure: Architecture of TrustLogin

TrustLogin

3 Steps for a password-login

- Entering secure input mode: Ctrl+Alt+1
- Intercepting keystrokes and generating placeholders
- Intercepting network packets

Case Study of TrustLogin

- Legacy Applications: FTP
  - Unencrypted packets
- Secure Applications: SSH
  - encrypted packets
  - session key searching
- TrustLogin requires application-specific efforts

Ensuring the Trust Path

Mitigating spoofing attacks

- LED lights:
  - Showing a special sequence of Num, Caps, and Scroll locks
  - User defines the sequence
- PC speaker:
  - Playing a melody (e.g., C major scale)

Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

Effectiveness of TrustLogin

- Testing TrustLogin against Keyloggers on Windows and Linux Platforms
  - Windows: Free Keylogger Pro version 1.0
  - Linux: Logkeys version 0.1.1a

  Keyloggers can only record random strings with TrustLogin enabled

Performance Evaluation

Table: Breakdown of TrustLogin Runtime

Operations	**Mean**	**STD**
Keyboard SMI handler	32.58 *ms*	3.68
NIC SMI handler	29.67 μs	1.18
SMM Switching	3.29 μs	0.08
SMM Resume	4.58 μs	0.10

Overview of The Talk

- Motivation
- Background: System Management Mode (SMM)
- System Framework
- Evaluation Results
- Conclusions and Future Directions

Conclusions and Future Directions

- We presented TrustLogin, a novel framework for securing password-login via System Management Mode
  - It can prevent rootkits from stealing sensitive data from the local host
  - It does not change any software on the client and server sides
  - It is transparent to users and applications
- Defend against phishing attacks by validating the destination IP/hostname
- Protect other sensitive data like password-logins on browsers and banking transactions

References I

[1] "Keylogger Malware Found on UC Irvine Health Center Computers," http://www.scmagazine.com/keylogger-malware-found-on-three-uc-irvine-health-center-computers/article/347204/.

[2] "Credit Card Data Breach at Barnes & Noble Stores," http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html?_r=3&.

[3] T. Holz, M. Engelberth, and F. Freiling, "Learning More About the Underground Economy: A Case-Study of Keyloggers and Dropzones," in *Proceedings of The 14th European Symposium on Research in Computer Security (ESORICS'09)*, 2009.

Thank you!

Email: fengwei@wayne.edu
Homepage: `http://fengwei.me`

Questions?