EPA-RIMM: Extensible, Performance-Aware SMM Runtime Integrity Measurement

Brian Delgado, Prof. Karen L. Karavanic

Portland State University

Goal

Extensible and Performance-Aware System Management Mode (SMM)-based runtime detection of kernel rootkits

- *Problem*: The unbounded SMM time and lack of extensibility of proposed techniques [2,3,4] for SMM-based runtime integrity checking are obstacles to their acceptance and use.
- *Our Approach*: Subdivide large inspections to reduce performance degradation, Create extensible framework to specify new inspections at runtime.
- *Conclusions*: EPA-RIMM allows controllable performance impact, more frequent measurements, and varied sets of measurements for each inspection.

Motivation

- The time to discover compromises is not keeping pace with the attacker's ability to quickly compromise systems. [1]
- New mechanisms needed to more quickly detect rootkits and alert on their presence
- Proposed SMM-based runtime integrity mechanisms [2,3,4] suffer from impractical performance overheads and lack of extensibility.

1. Verizon 2016 Data Breach Investigations Report
2. Azab, A., Ning, P., Wang, Z., Jiang, X., Zhang X., Skalsky, N. "HyperSentry: enabling stealthy in-context measurement of hypervisor integrity," CCS. Chicago, IL, 2010.
3. Wang, J., Stavrou, A., Ghosh, A. "HyperCheck: a hardware-assisted integrity monitor," Lect. Notes Comput. Sci. Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics) 6307 LNCS: 158-177, 2010.
4. Zhang, F., Leach, K. Sun, K., Stavrou, A. "SPECTRE: A Dependable Introspection Framework via System Management Mode, 43rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Budapest, Hungary, 2013

Research Challenges

- Methods of supporting extensible measurements when "pristine" measurements unavailable
- Specification of more advanced measurements, including hypervisor inspections
- Supporting effective and stealthy out-of-band communication to SMM-based Inspector

Future Work

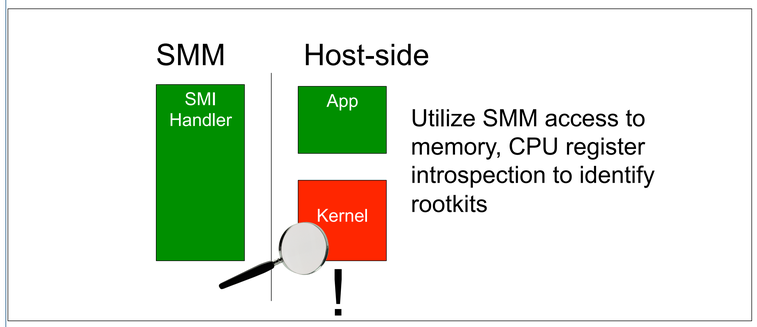
- Develop simulator for EPA-RIMM scheduler to evaluate options of scheduling large numbers of tasks
- Develop SMM benchmarks for runtime integrity measurement (hash, encryption)
- Enable hypervisor inspections
- Allow incoming threat data to drive new inspections. Share discovered threats via STIX [1] (or similar)

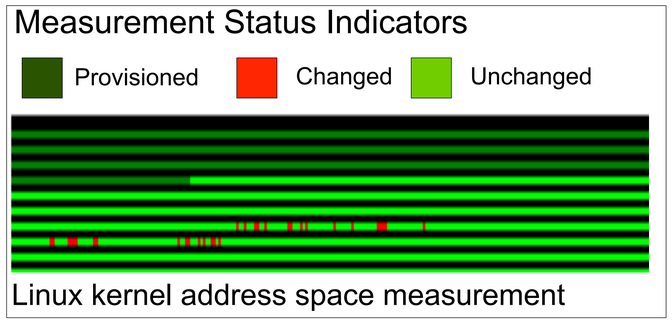
1. STIX, https://stixproject.github.io

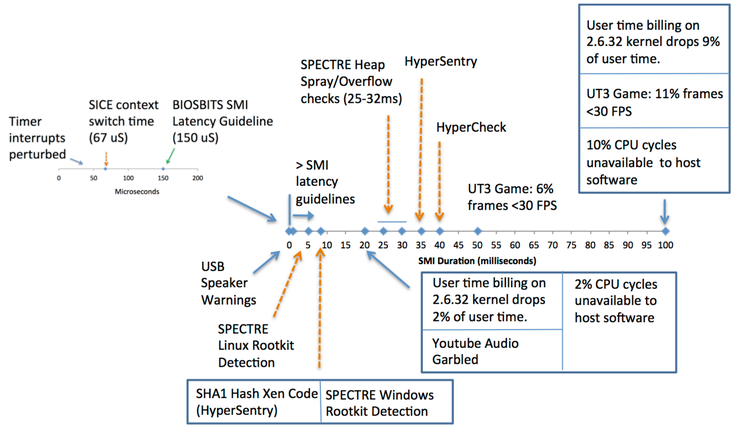
Contact

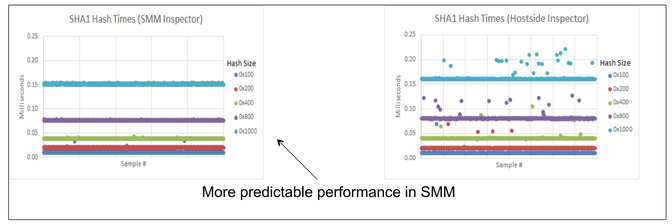
{ bdelgado, karavan } @ pdx.edu

SMM-based Rootkit Detection (RIMM)









Extensible Checks

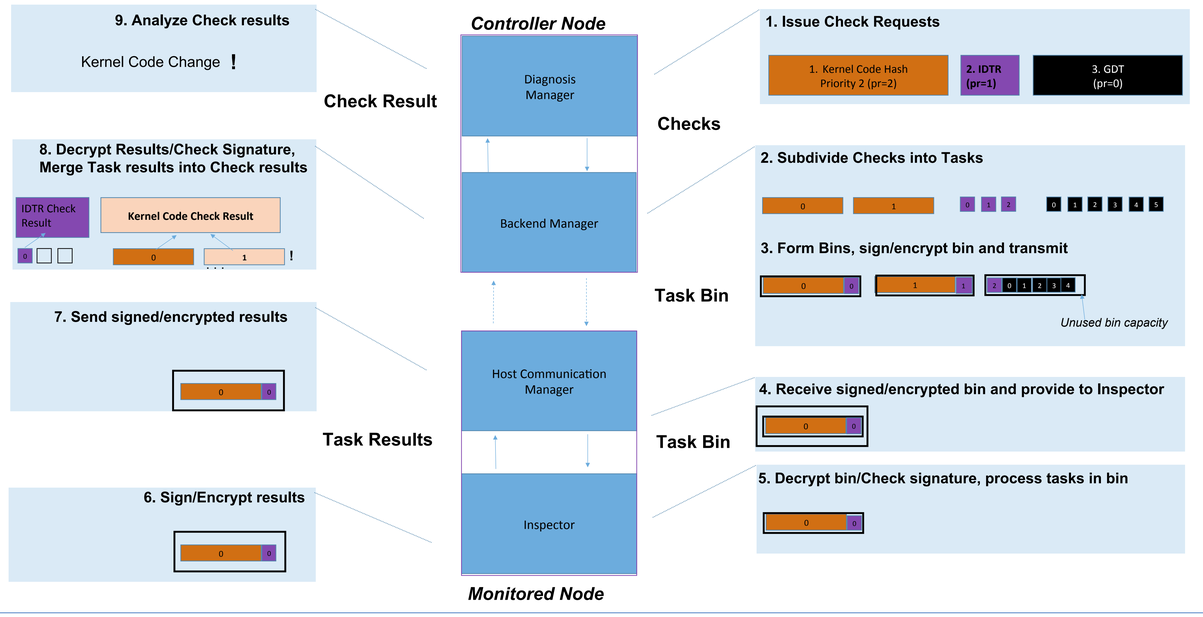
Check Description
Check ID #
Command
Operand
Memory Address
Length
Subdivision Target
Time of last check
Check Priority

Command	Selected Parameters
Measure Register	CR0,CR3 , CR4,IDTR,GDTR
Measure Virt Mem	Address, Length
Measure Phys Mem	Address, Length
Measure MSR	MSR Number

Key Insight:

We can apply techniques from the Operating System to System Management Mode Integrity Checks

How? Break down security inspections into smaller tasks, Schedule fixed-length bins of tasks, Maintain a limit on time in SMM



Acknowledgments

This work was supported in part by NSF Award #1528185

John Fastaband, Mitch Souders, Konstantin Macarenco, Kristina Frye contributed ideas, discussions, and experiments included in this work.