Micro-Virtualization Memory Tracing to Detect and Prevent Spraying Attacks

Stefano Cristalli, Mattia Pagnozzi, Mariano Graziano,
Andrea Lanzi, Davide Balzarotti

Universita' degli Studi di Milano
Cisco Systems, Inc.
Eurecom

USENIX Security 2016 - Austin, USA

TaLOS

SPRAYING

- Traditional code based spraying
- JIT spraying
- Data spraying and stack pivoting

RELATED WORK

HEAP SPRAYING

- Egele et al. - DIMVA 09
- Nozzle - USENIX Security 09
- BuBBLE - ESSoS 10

RELATED WORK

HEAP SPRAYING

- Egele et al. - DIMVA 09
- Nozzle - USENIX Security 09
- BuBBLE - ESSoS 10

JIT SPRAYING

- JITsec - VEE 06
- Bania - Whitepaper 10
- JITDefender - IFIP 11
- Lobotomy - Ares 14

RELATED WORK

HEAP SPRAYING

- Egele et al. - DIMVA 09
- Nozzle - USENIX Security 09
- BuBBLE - ESSoS 10

JIT SPRAYING

- JITsec - VEE 06
- Bania - Whitepaper 10
- JITDefender - IFIP 11
- Lobotomy - Ares 14

DATA SPRAYING

- EMET - Microsoft 09
- Browser solutions

RELATED WORK

HEAP SPRAYING

- Egele et al. - DIMVA 09
- Nozzle - USENIX Security 09
- BuBBLE - ESSoS 10

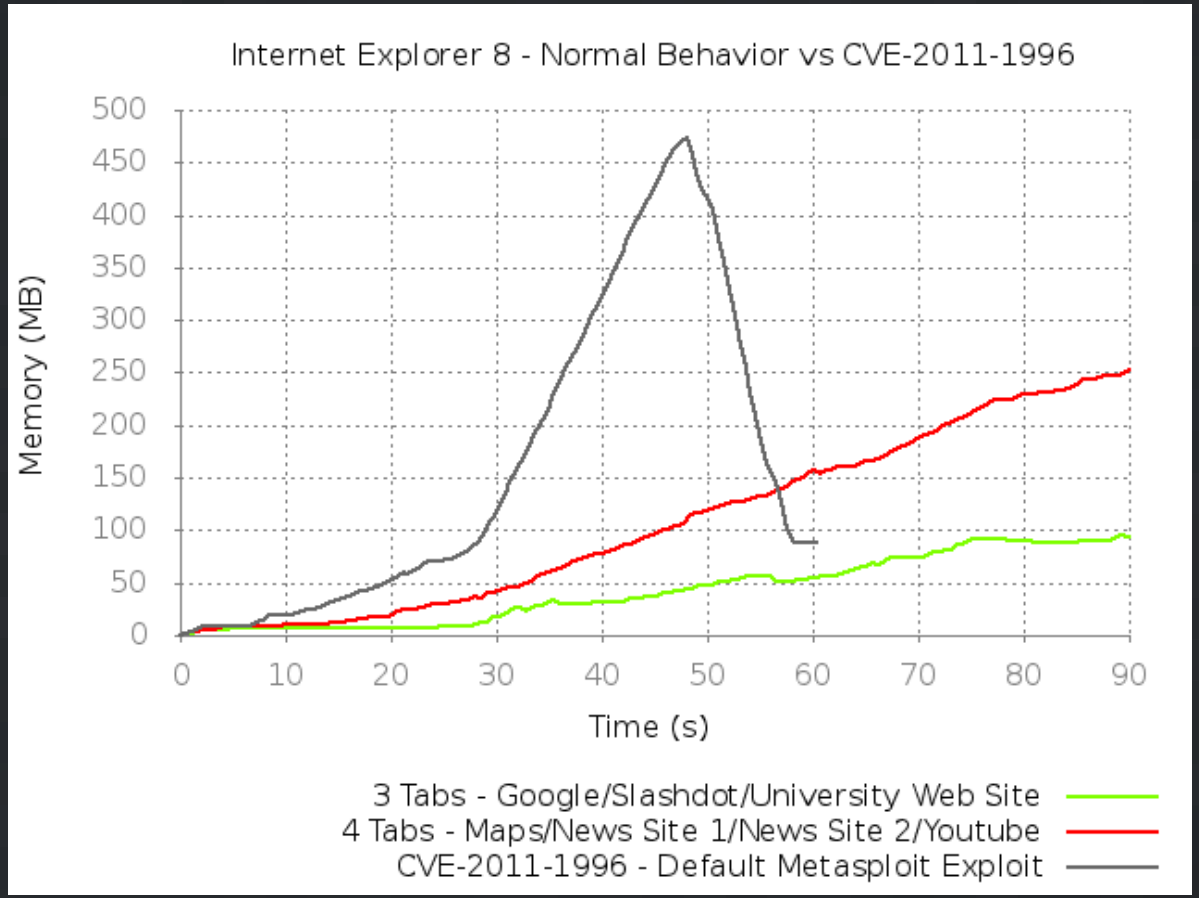
- No comprehensive and scalable solutions vs spraying
- No OS agnostic solutions

- Bania - Whitepaper 10
- JITDefender - IFIP 11
- Lobotomy - Ares 14

DATA SPRAYING

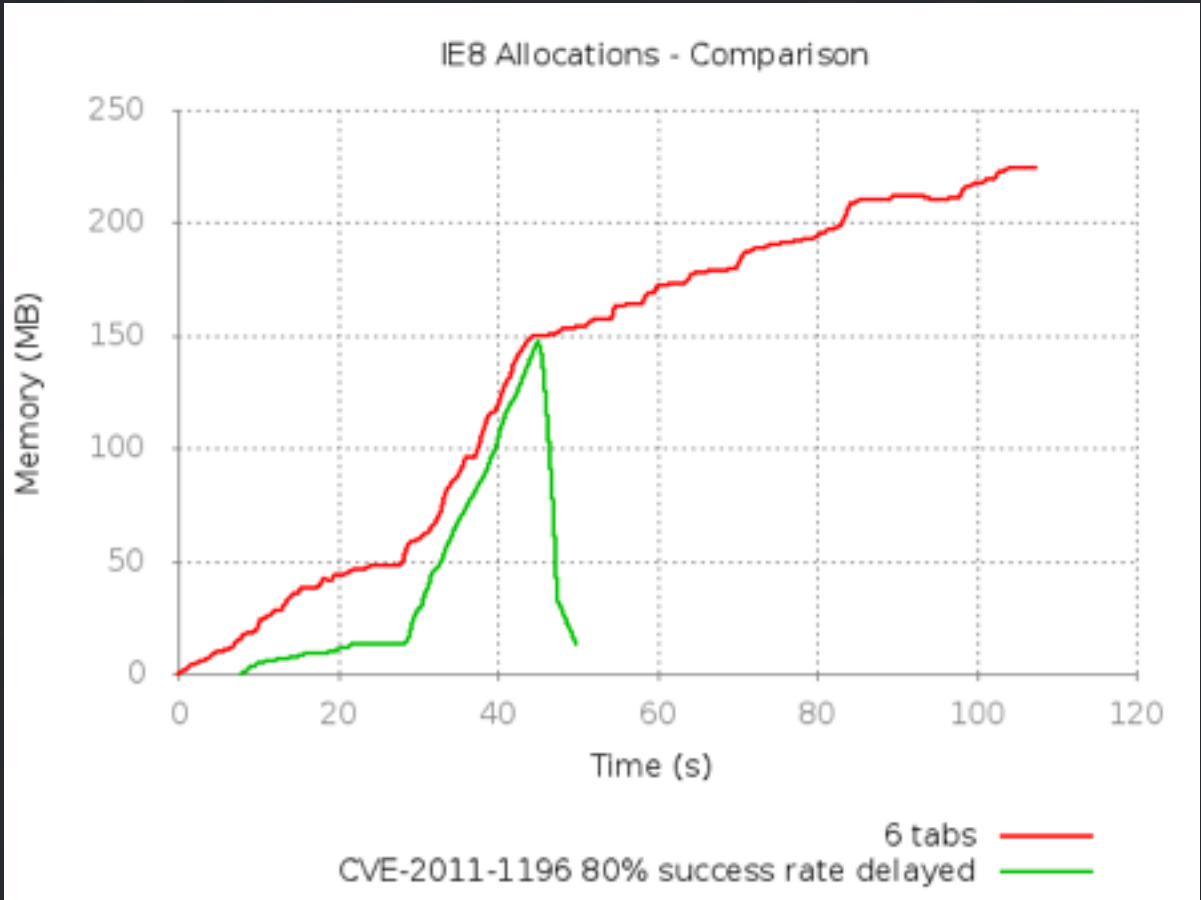
- EMET - Microsoft 09
- Browser solutions

MEMORY FOOTPRINT



TALOS

MEMORY FOOTPRINT



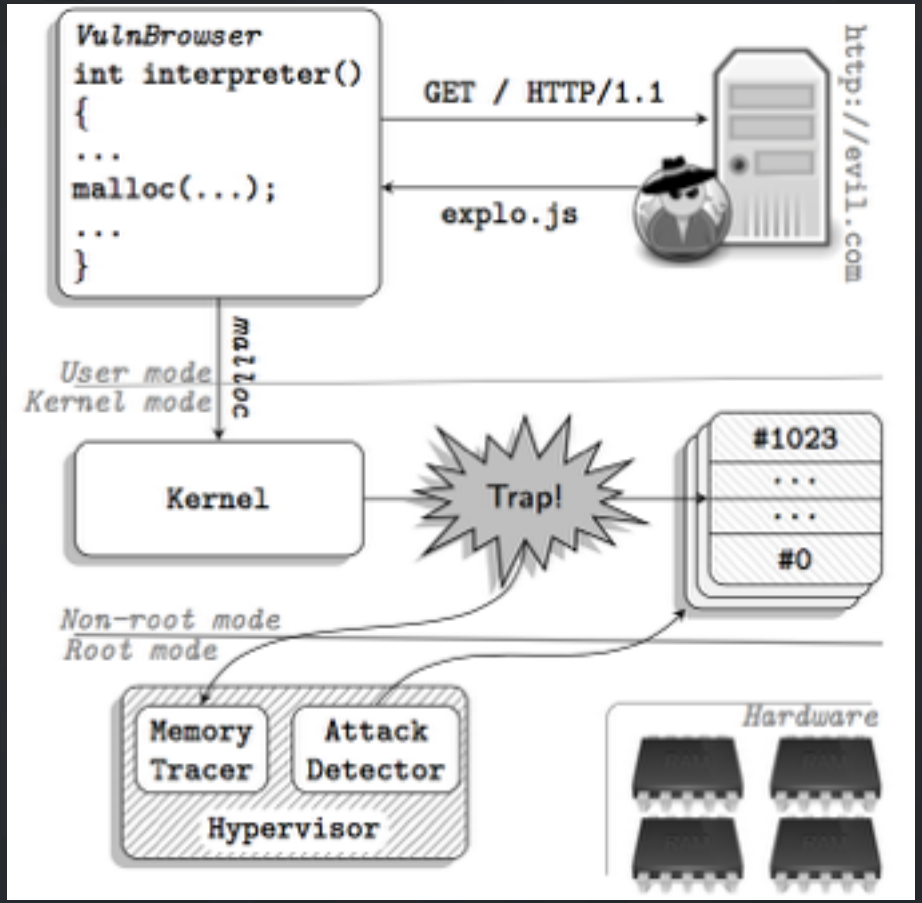
TALOS

GOALS

- The system should be completely independent from the memory allocator used by the protected application
- The system should not require any OS dependent information
- The overhead introduced by our system should be "reasonable"
- Modular framework based on plugins

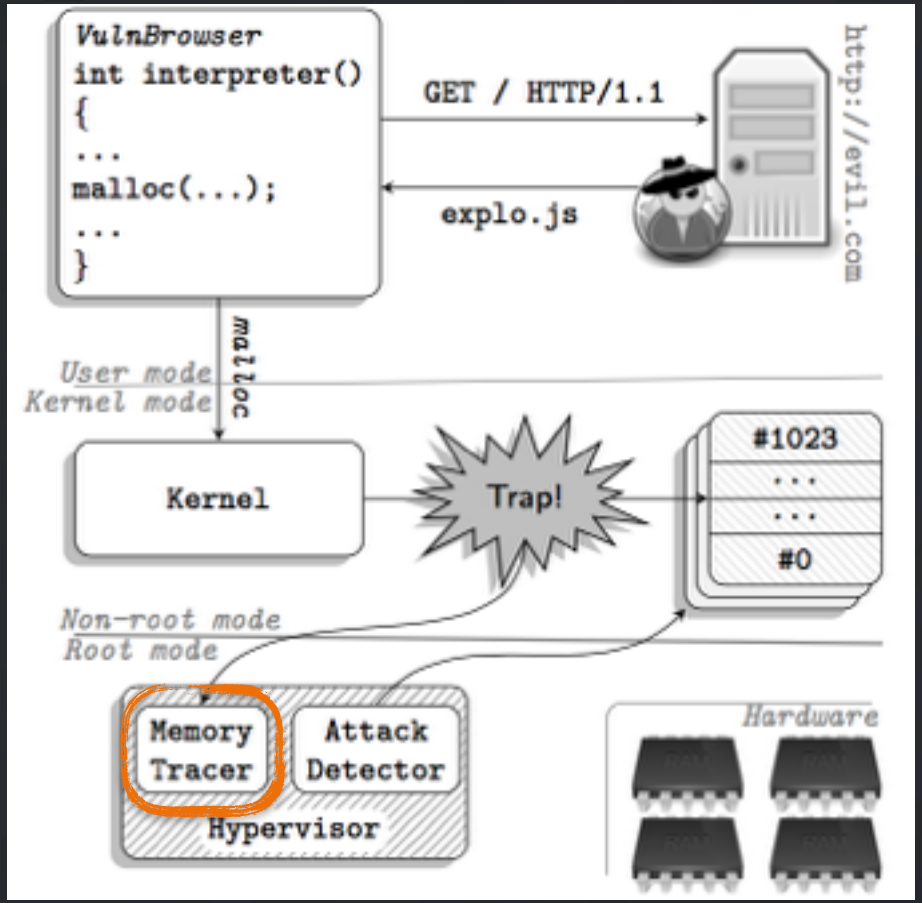
TALOS

ARCHITECTURE OVERVIEW



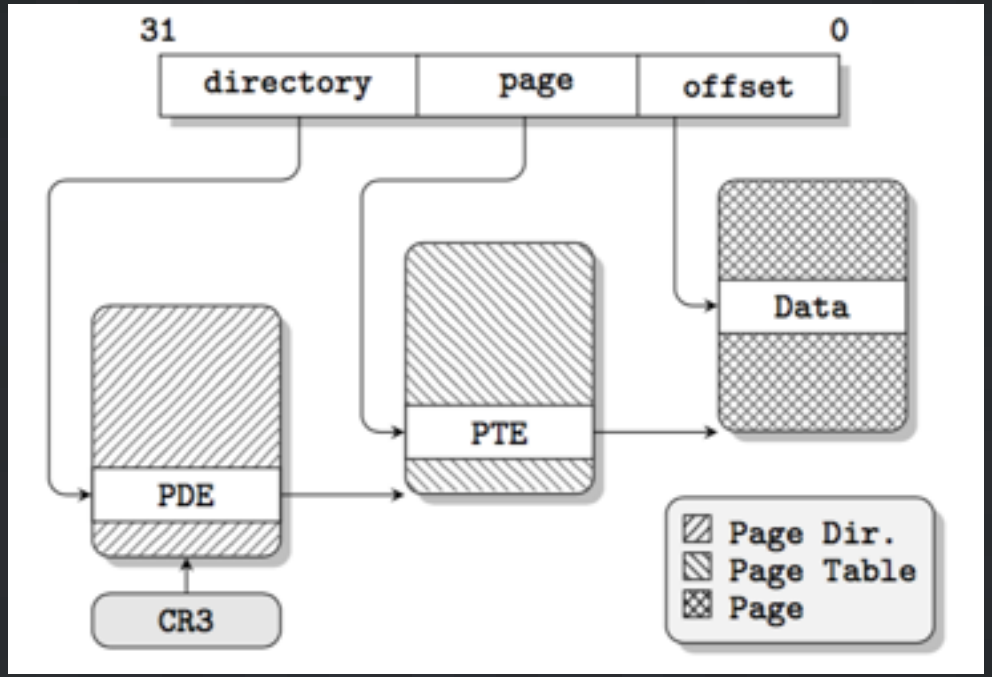
TALOS

ARCHITECTURE OVERVIEW



TALOS

MEMORY TRACER



Creation/Modification/Removal of the page: Detected by looking at the PTE
Creation/Modification/Removal of the page table: Detected by looking at the PDE

TALOS

INTERFERENCE PROBLEM

- Overhead issues:
  - A modification of the memory page of the running process creates a side effect modification of a memory page in another process
  - Due to kernel memory operations optimizations

TALOS

INTERFERENCE PROBLEM

- Overhead for Internet Explorer 10 (IE): 22%
- Overhead for Acrobat Reader and Firefox on top of IE: 63%
- IE's overhead increases from 22% to 63%

MICRO-VIRTUALIZATION

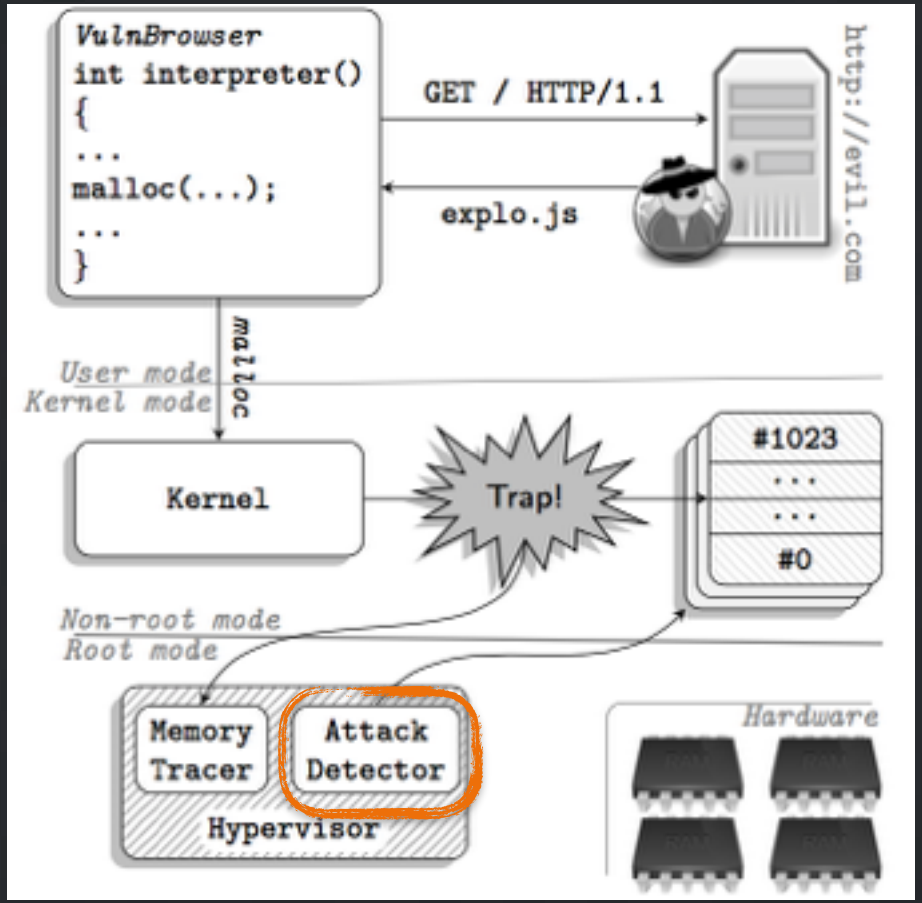
- Each monitored process runs inside its own virtual memory sandbox

- Graffiti enables the memory protection only for the actual running and monitored process

MICRO-VIRTUALIZATION: DETAILS

- Micro-virtualization is based on EPT:
  - Select a set of physical pages to monitor the target process
  - One EPT pointer (EPTP) per process

ARCHITECTURE OVERVIEW



TALOS

STATIC ANALYZER

- Set of heuristics to detect the different spraying techniques:
  - Malicious code detector [ACSAC10, SEC11]

STATIC ANALYZER

- Set of heuristics to detect the different spraying techniques:
  - Malicious code detector [ACSAC10, SEC11]
  - Self-unpacking shellcode detector [ACSAC07]

TALOS

STATIC ANALYZER

- Set of heuristics to detect the different spraying techniques:
  - Malicious code detector [ACSAC10, SEC11]
  - Self-unpacking shellcode detector [ACSAC07]
  - Data spraying detector [RAID13,RAID15]

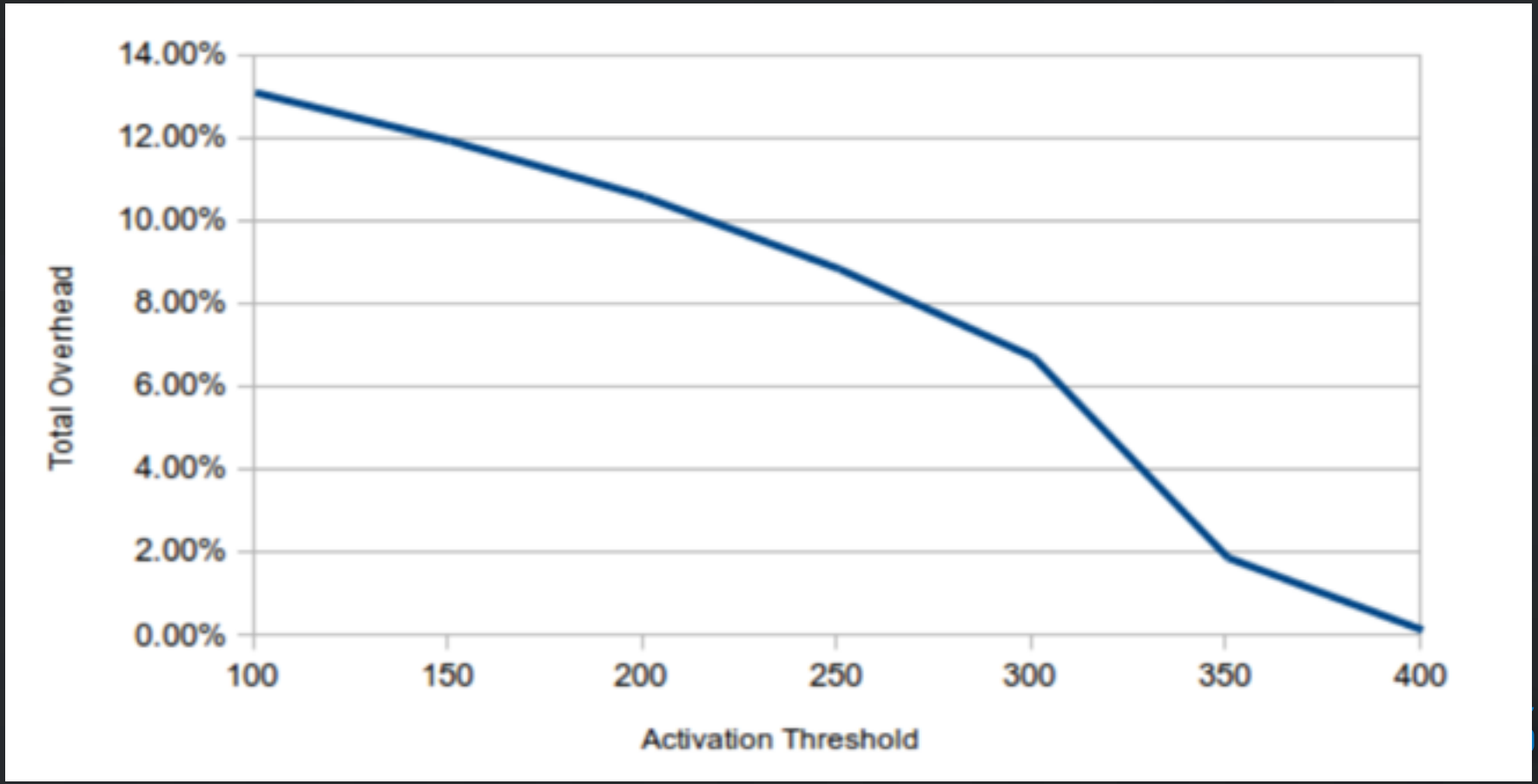
TALOS

EXPERIMENTS: OVERHEAD

- The memory tracer is always active
- Stress suite results (8MB every 2s):
  - Windows 7: 24%
  - Linux 3.2: 25%

TALOS

EXPERIMENTS: OVERHEAD



DETECTION ACCURACY

CVE	Application	Exploit Technique	Detected
2010-0248	Adobe Flash player	ROP + packed sc	Yes
2011-0609	Adobe Reader	JIT + packed sc	Yes
2011-2462	Adobe Reader	ROP + packed sc	Yes
2010-2883	Adobe Reader	Ret2Lib + packed sc	Yes
2011-1996	IExplorer	ROP	Yes
2009-2477	Firefox	Plain Shellcode	Yes

TALOS

DETECTION ACCURACY

- System tested also with 1000 malicious PDF, 1000 benign PDF documents and top 1000 Alexa websites
- Conservative threshold (150MB)
- Graffiti detected all the attacks with zero false alarms

TALOS

GLOBAL EXPERIMENTS

- Final global test in which real users use Graffiti during their everyday activities for a total of 8-10 hours per day in a period of 7 days

- Conservative threshold of 150MB on IE8 for Windows 7 machines

TALOS

GLOBAL EXPERIMENTS

- 492 distinct web pages visited
- Detectors activated 55 times (~8 times per day)
- 12 alerts on pages that seemed to be benign. A closer inspection of the false positive shows the data spraying detector to be the only responsible

CONCLUSIONS

- First efficient and comprehensive solution to defeat spraying
- Micro-virtualization
- Open source

TALOS

SOURCE CODE

Code available at

https://github.com/graffiti-hypervisor/graffiti-hypervisor

TALOS

QUESTIONS?

Mariano Graziano
magrazia@cisco.com
@emd3l

