The Impact of GPU-Assisted Malware on Memory Forensics: A Case Study

By

Davide Balzarotti, Roberto Di Pietro and Antonio Villani

Presented At

The Digital Forensic Research Conference

DFRWS 2015 USA Philadelphia, PA (Aug 9th - 13th)

The Impact of GPU-Assisted Malware on Memory Forensics: A Case Study

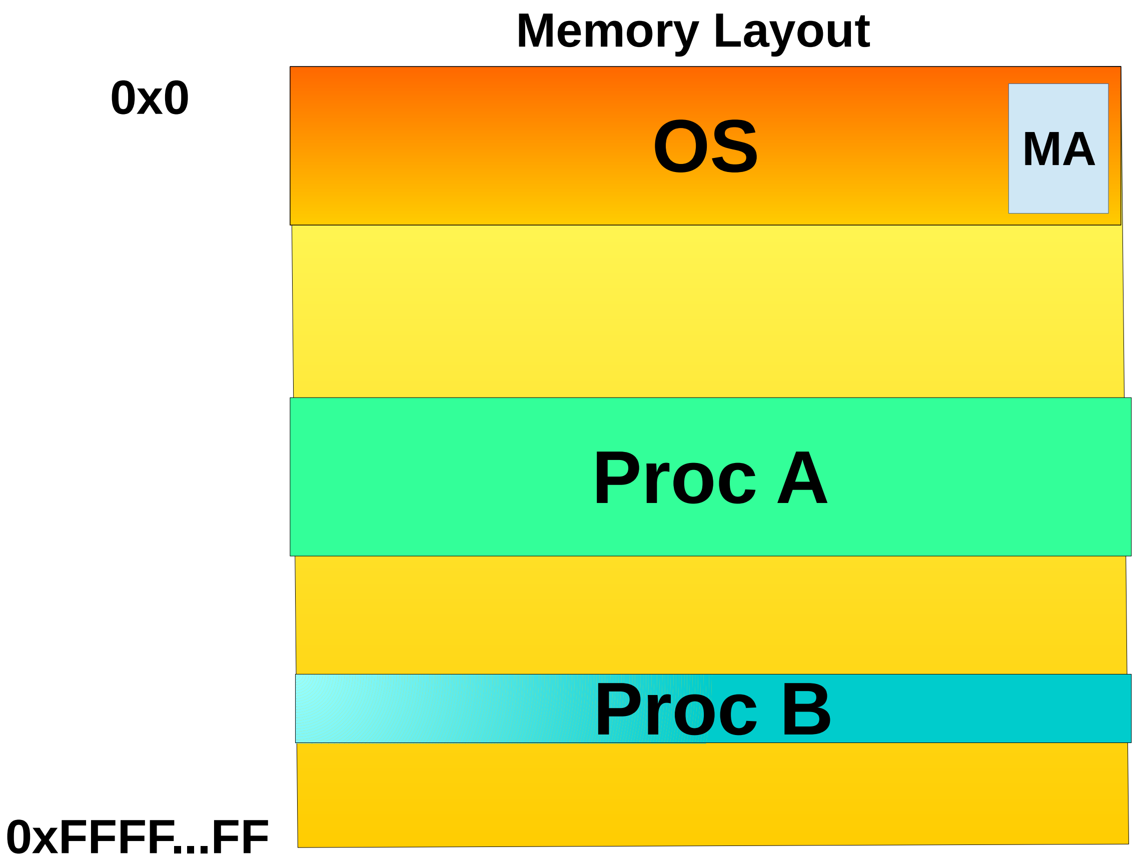
D.Balzarotti[a], *R. Di Pietro*[b] *and* ***A. Villani***[b]

[a]EURECOM, Sophie Antipolis, France
[b]University of Roma Tre, Rome, Italy

davide.balzarotti@eurecom.fr,
{dipietro,villani}@mat.uniroma3.it

***DFRWS USA 2015 Annual Conference*, Philadelphia**

Software memory acquisition

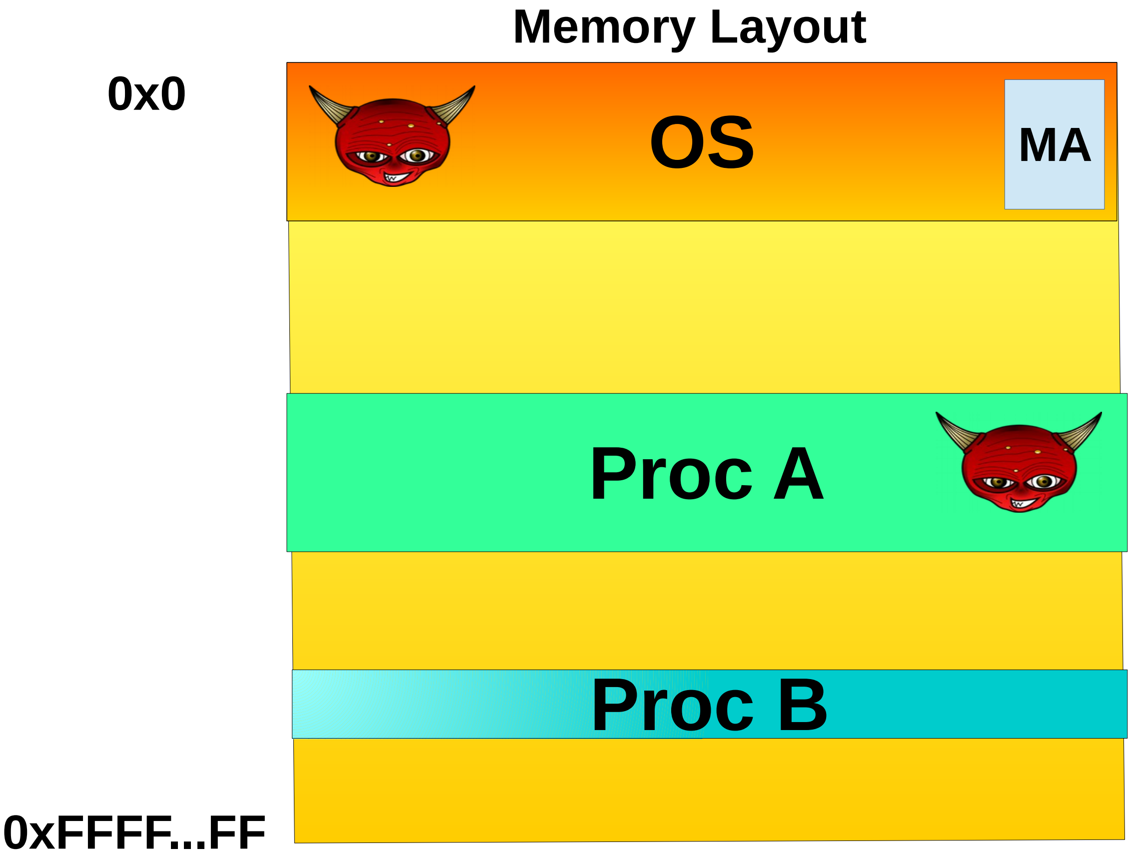


Memory Acquisition

1)For each **page** in **pages**

a)Read **p** from memory
b)Write **p** to disk

Software memory acquisition

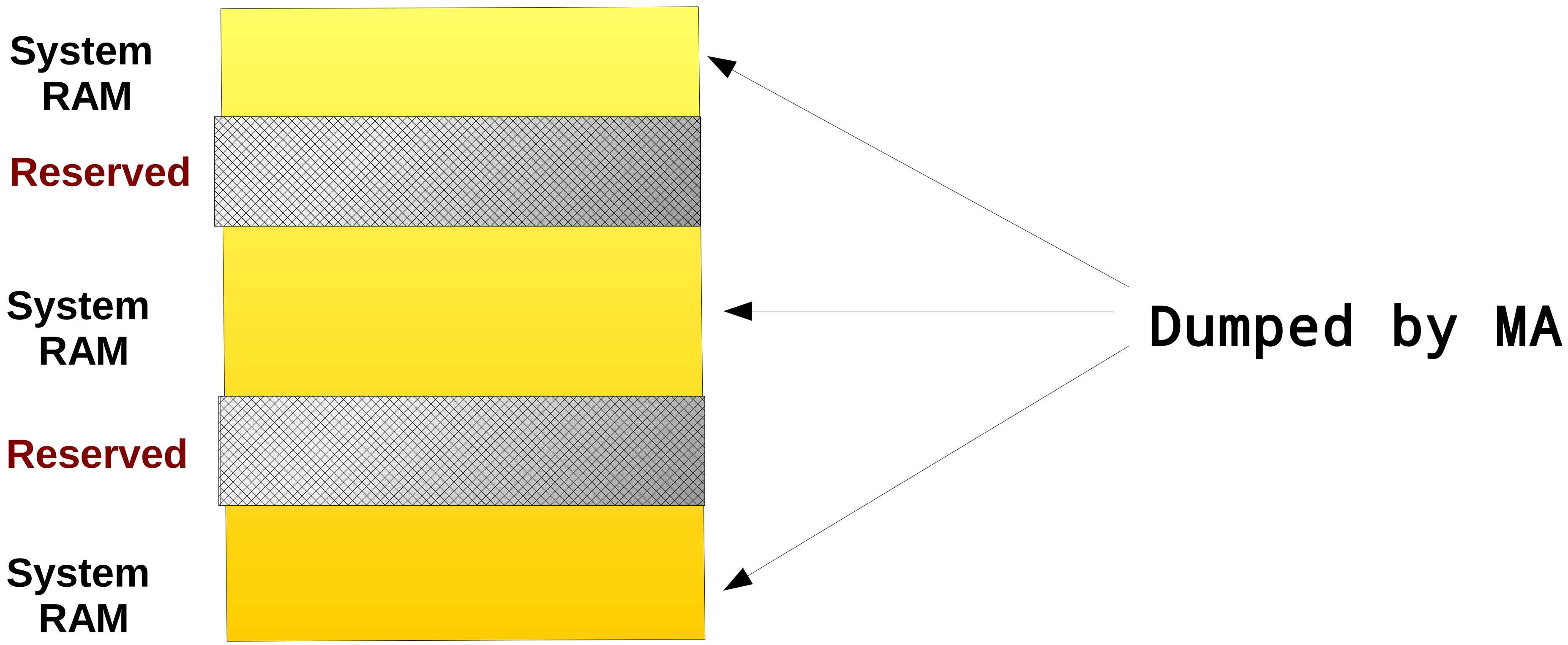


Memory Acquisition

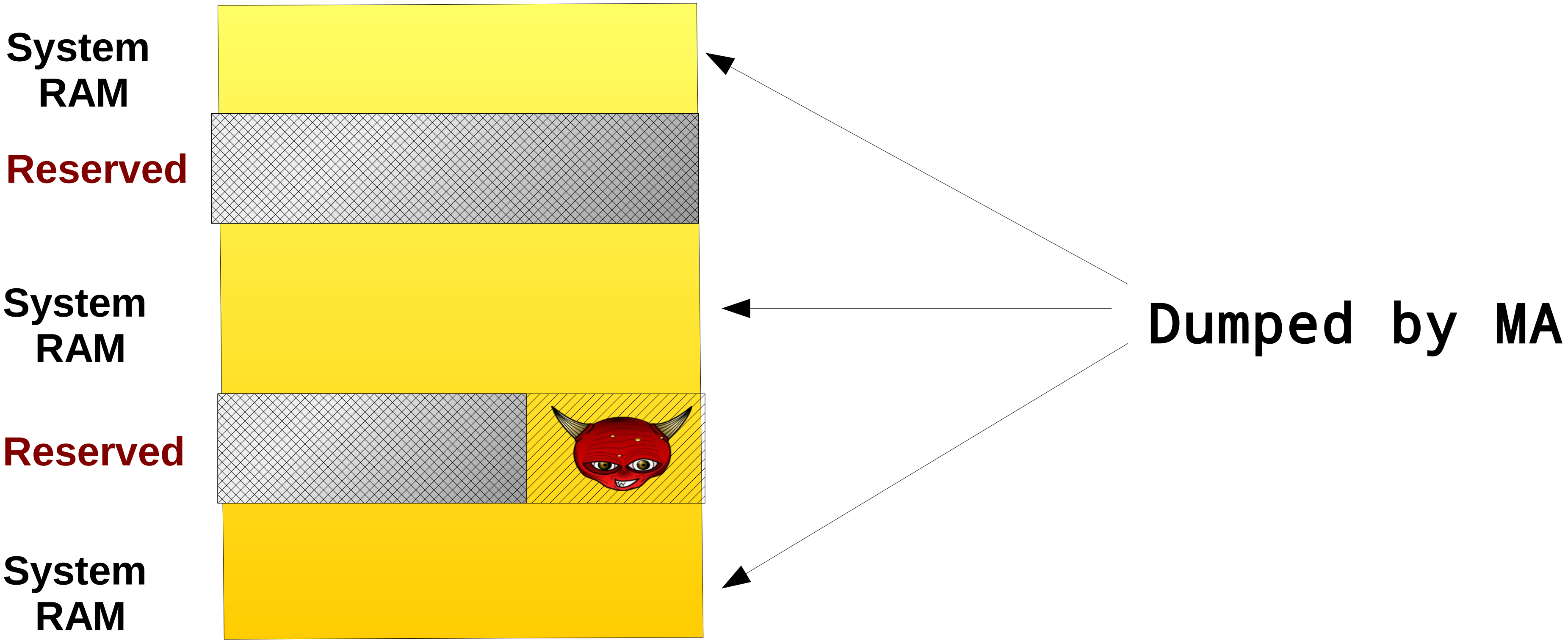
```
1)For each page in pages

  a)Read p from memory
  b)Write p to disk
```

Real Memory Layout

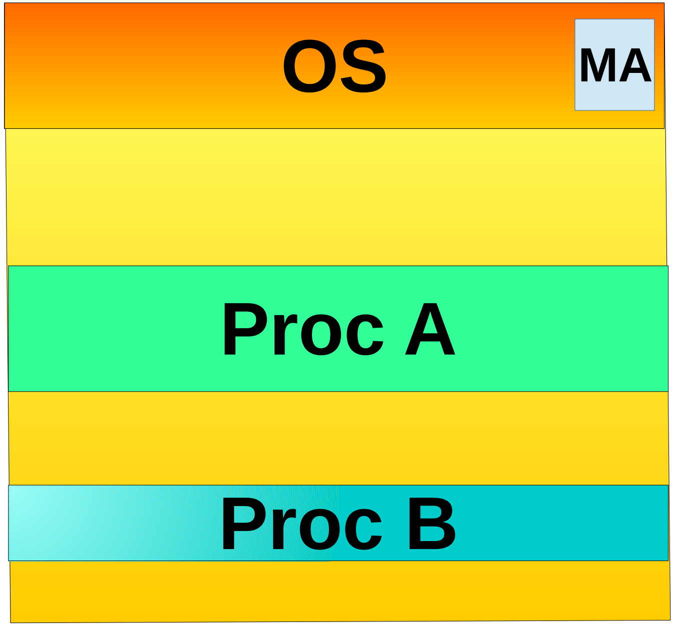


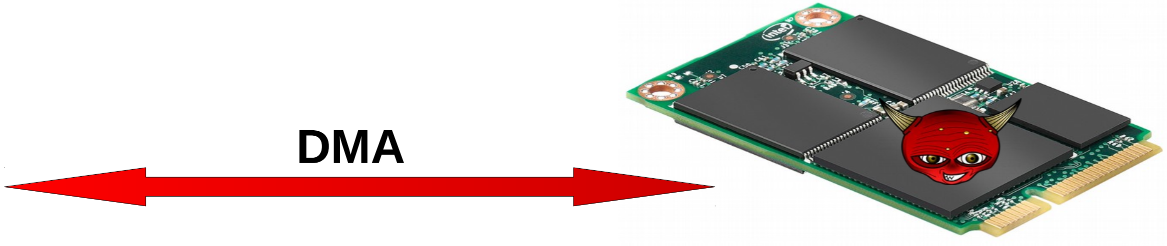
Passive Anti-forensic techniques*

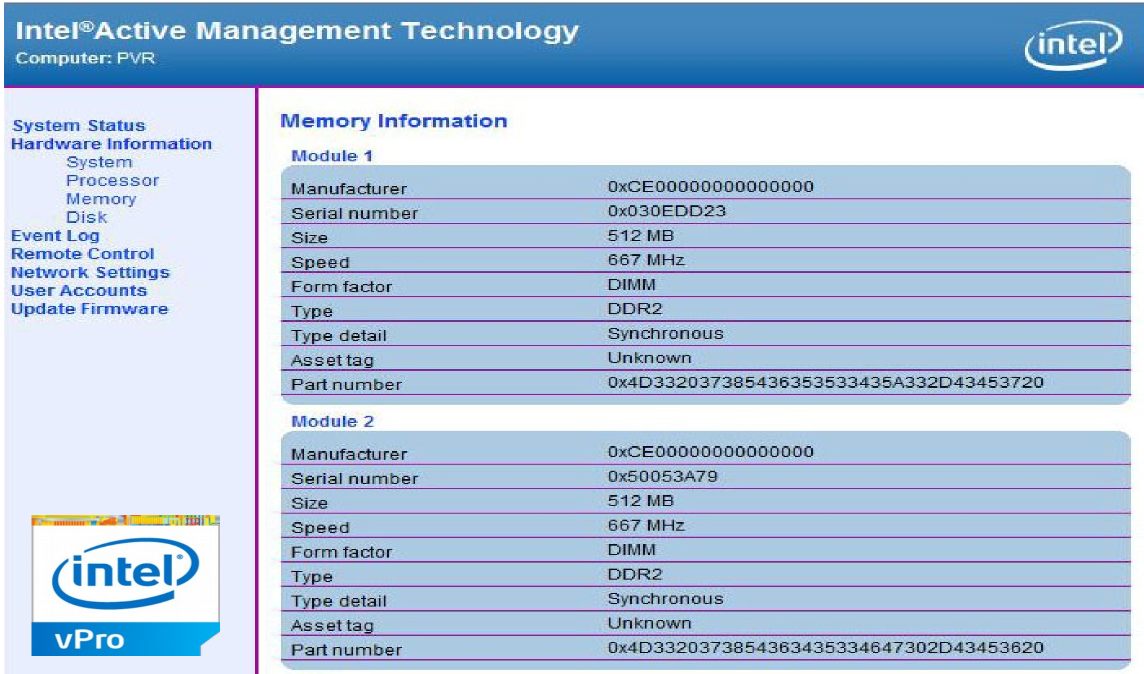


* Stuttgen, J., Cohen, M., *Anti-forensic resilient memory acquisition* – DFRWS 2013

DMA malware*







Module 1

Manufacturer	0xCE00000000000000
Serial number	0x030EDD23
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D332037385436353533435A332D43453720

Module 2

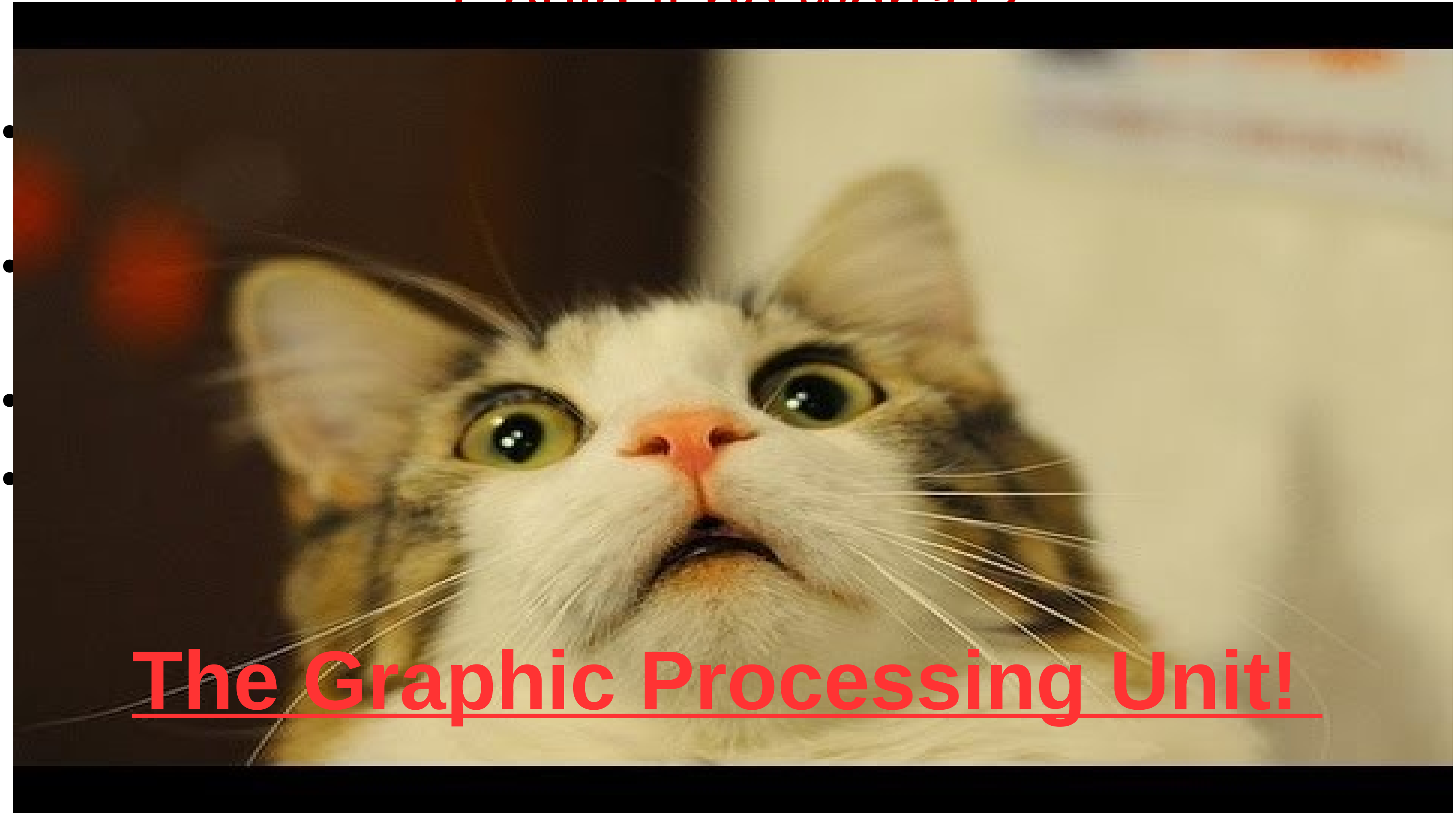
Manufacturer	0xCE00000000000000
Serial number	0x50053A79
Size	512 MB
Speed	667 MHz
Form factor	DIMM
Type	DDR2
Type detail	Synchronous
Asset tag	Unknown
Part number	0x4D3320373854363435334647302D43453620

* P. Stewin, *Understanding DMA Malware,* DIMVA 2013

Could it be worse?

- Of course, yes! ;-)
- Think about an "*external*" device that is (w.r.t. AMT):
  - more pervasive
  - more essential for the system
  - with more computational power
  - with a big *reserved* memory
  - easy to program
  - not supported/considered by current anti-virus software
- What can be such device?

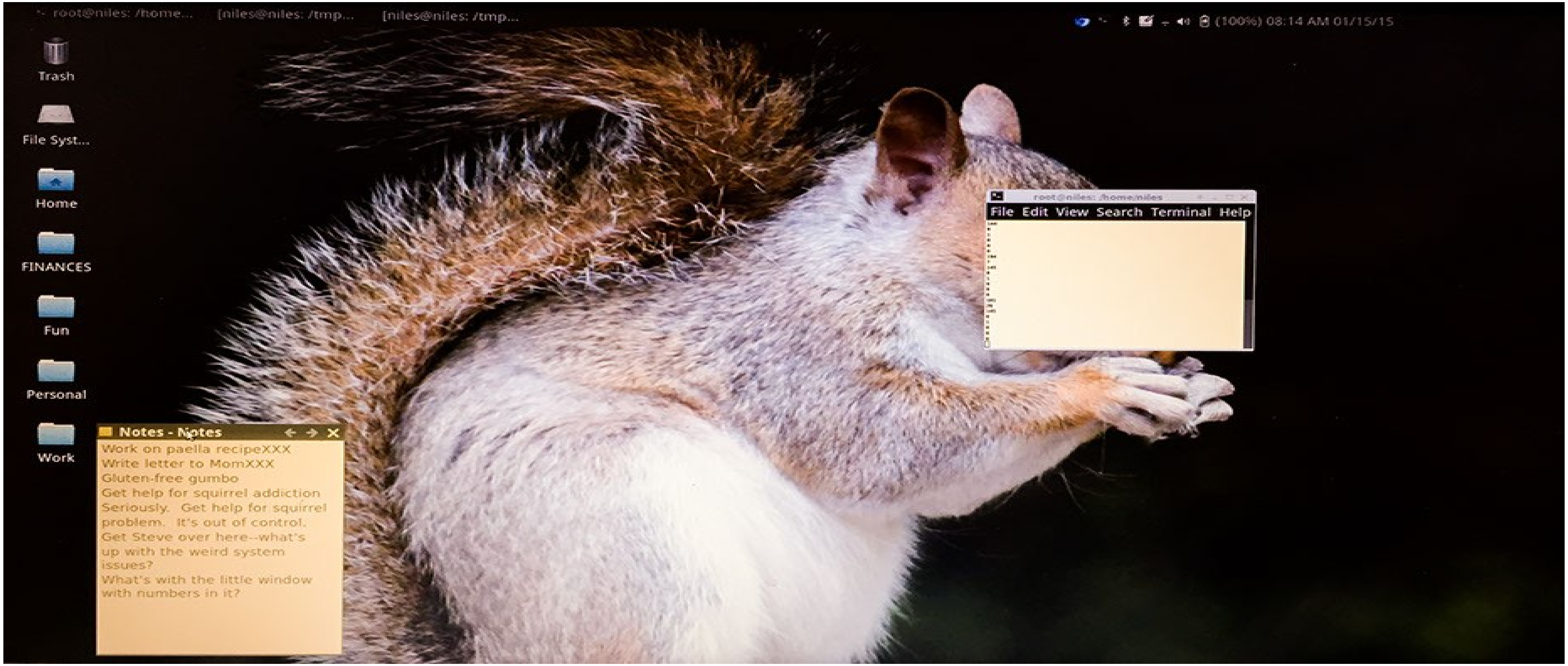
Could it be worse?



The GPU threat

- Almost every server/laptop/smartphone has one GPU (at least)
  - Some even have multiple GPUs (e.g. optimus technology)
- GPUs:
  - are fundamental for any system that runs a GUI
  - can be easily programmed with OpenCL / CUDA / APP
  - are equipped with GBs of reserved/dedicated RAM
  - have great computational capabilities
  - ABI is not supported by anti-virus

It got the attention of the DF community...



...and media

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

Ars Technica has arrived in Europe. **Check it out!**

RISK ASSESSMENT / SECURITY & HACKTIVISM

GPU-based rootkit and keylogger offer superior stealth and computing power

Proof-of-concept malware may pave the way for future in-the-wild attacks.

by **Dan Goodin** - May 7, 2015 5:43pm CEST

Share Tweet 61

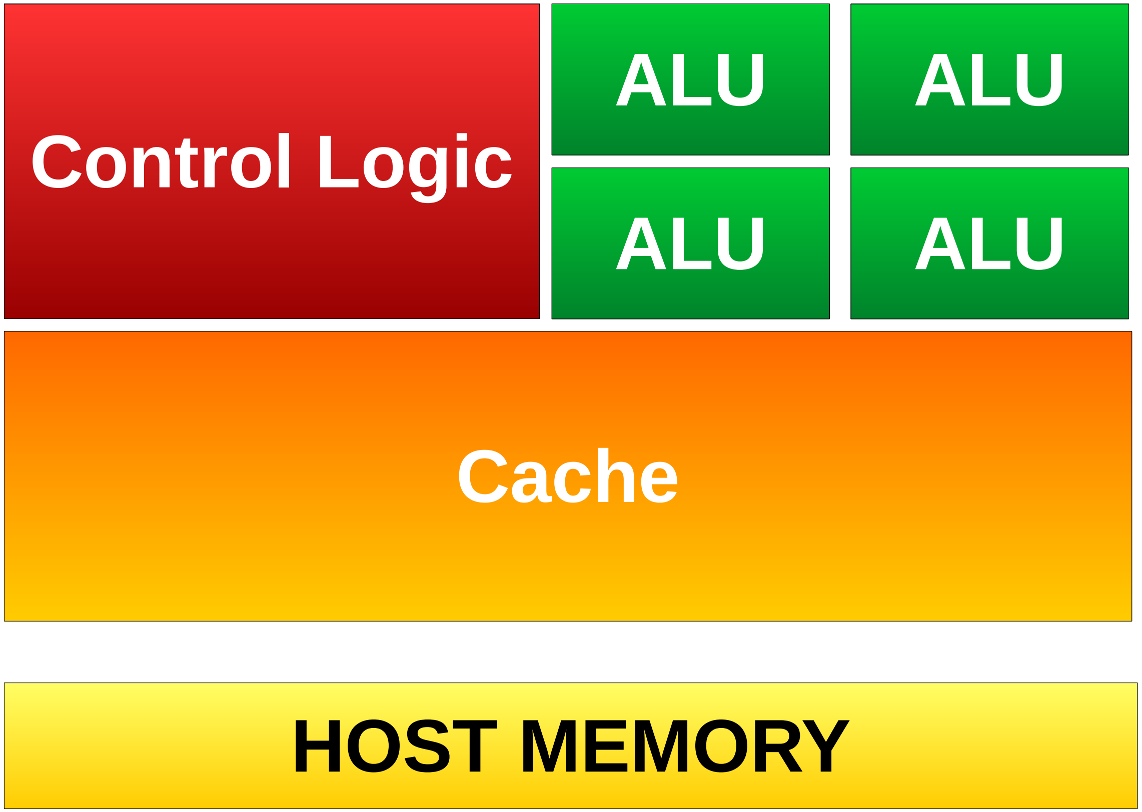
Contributions

- Model the GPU malware from a memory-forensic perspective
- Identify which artifacts can/should be collected for an effective DF investigation
- Provide a case study for Intel GPUs
- Show novel GPU anti-forensics techniques

Outline

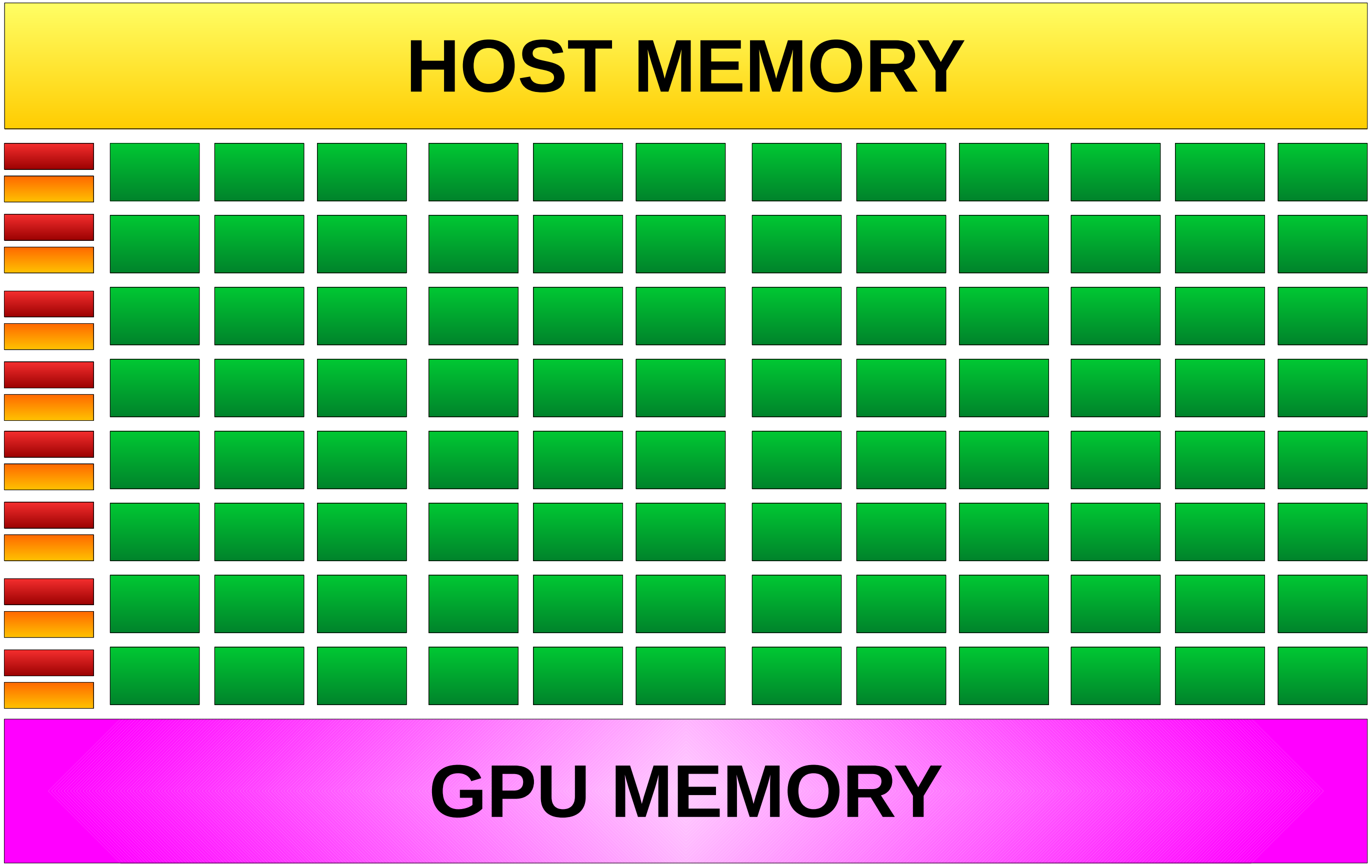
I. ~~Motivation~~
II. Background
III. GPU-assisted malware
IV. Case study: Intel Integrated GPUs
V. Conclusion

CPU



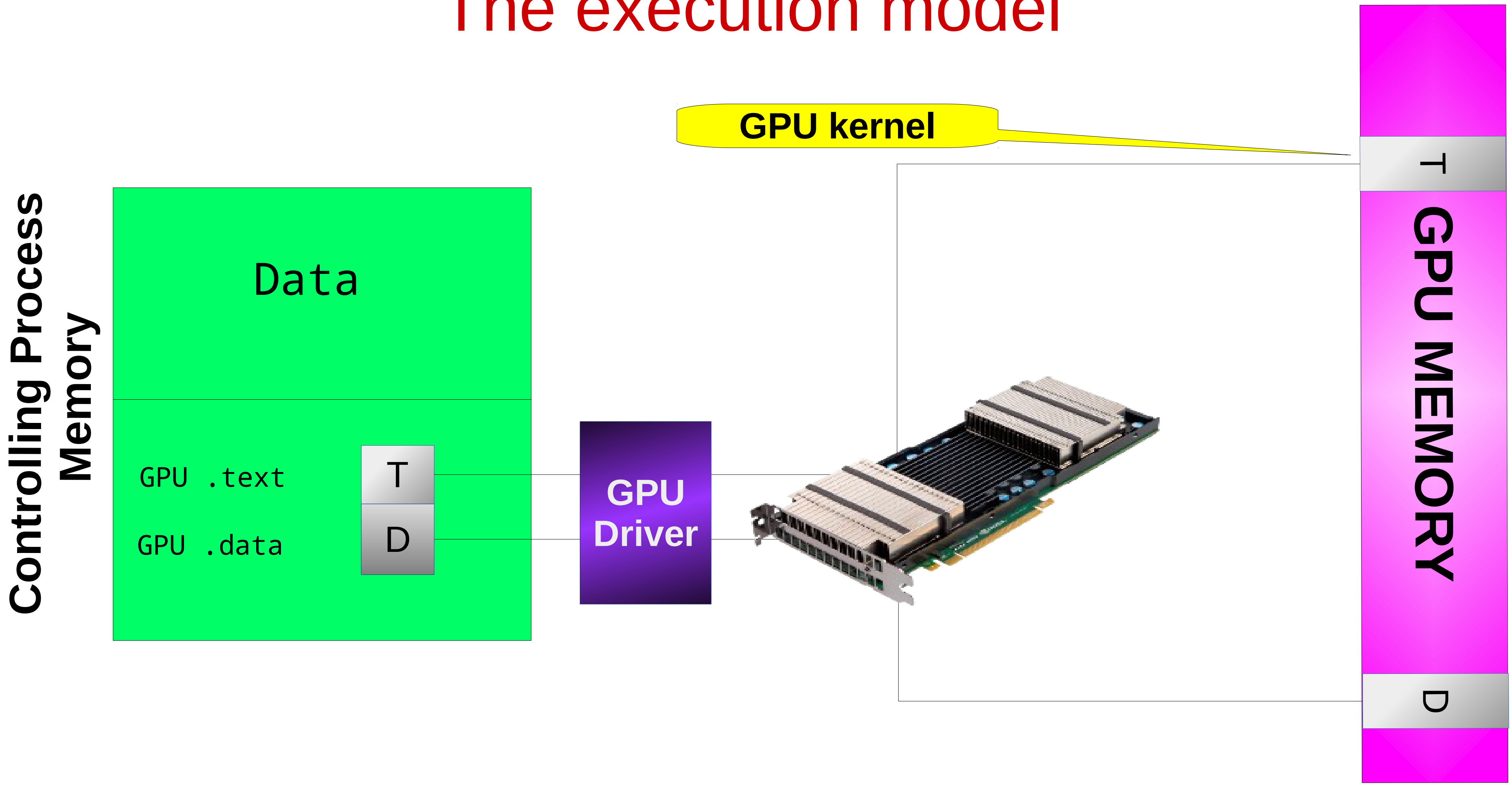
1) Few ALUs (e.g. 4,8,16)
2) Complex control Logic
   - Speculative execution
   - Branch prediction
3) Cache
   1) Shared LLC
   2) Per-core cache (smaller)

GPU

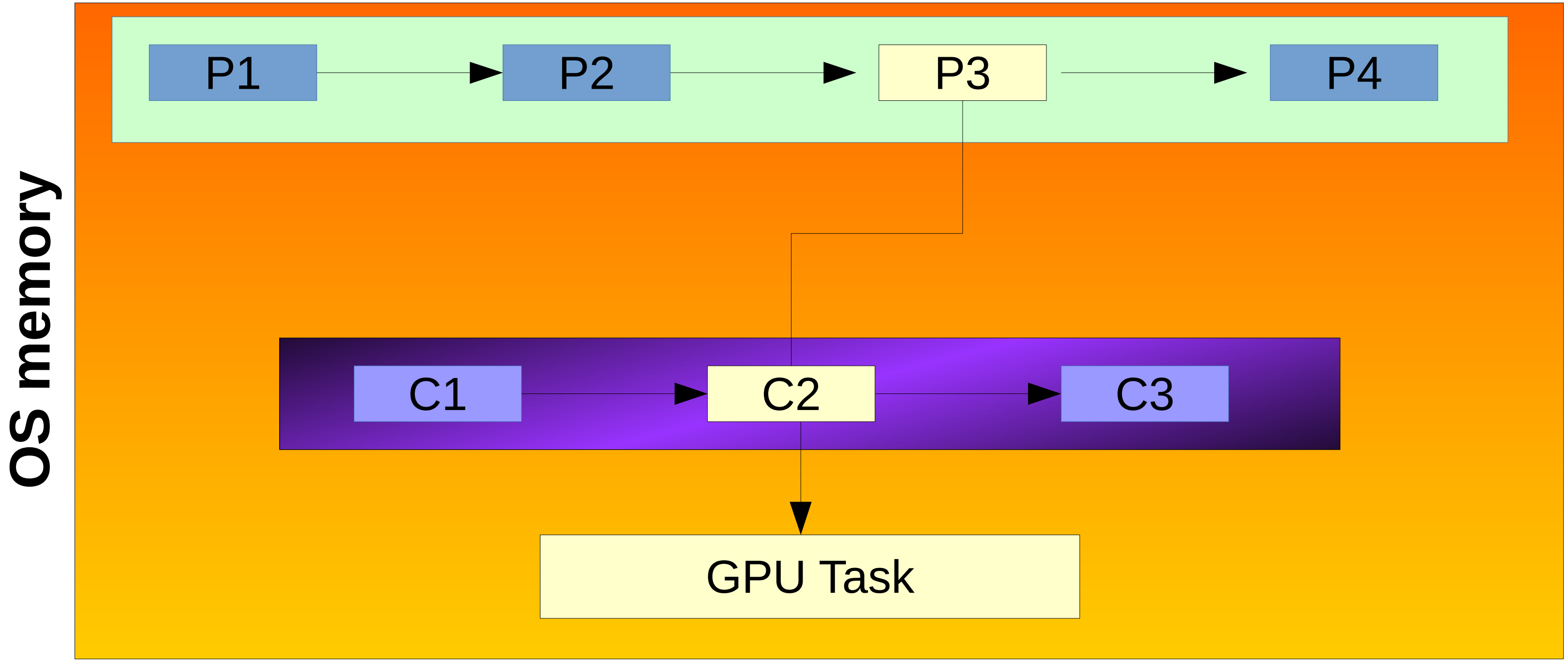


1) Many ALUs (hundreds)
2) Simple control Logic
   - e.g. Divergent execution paths get serialized
3) Very small Cache

The execution model



Process and Context lists



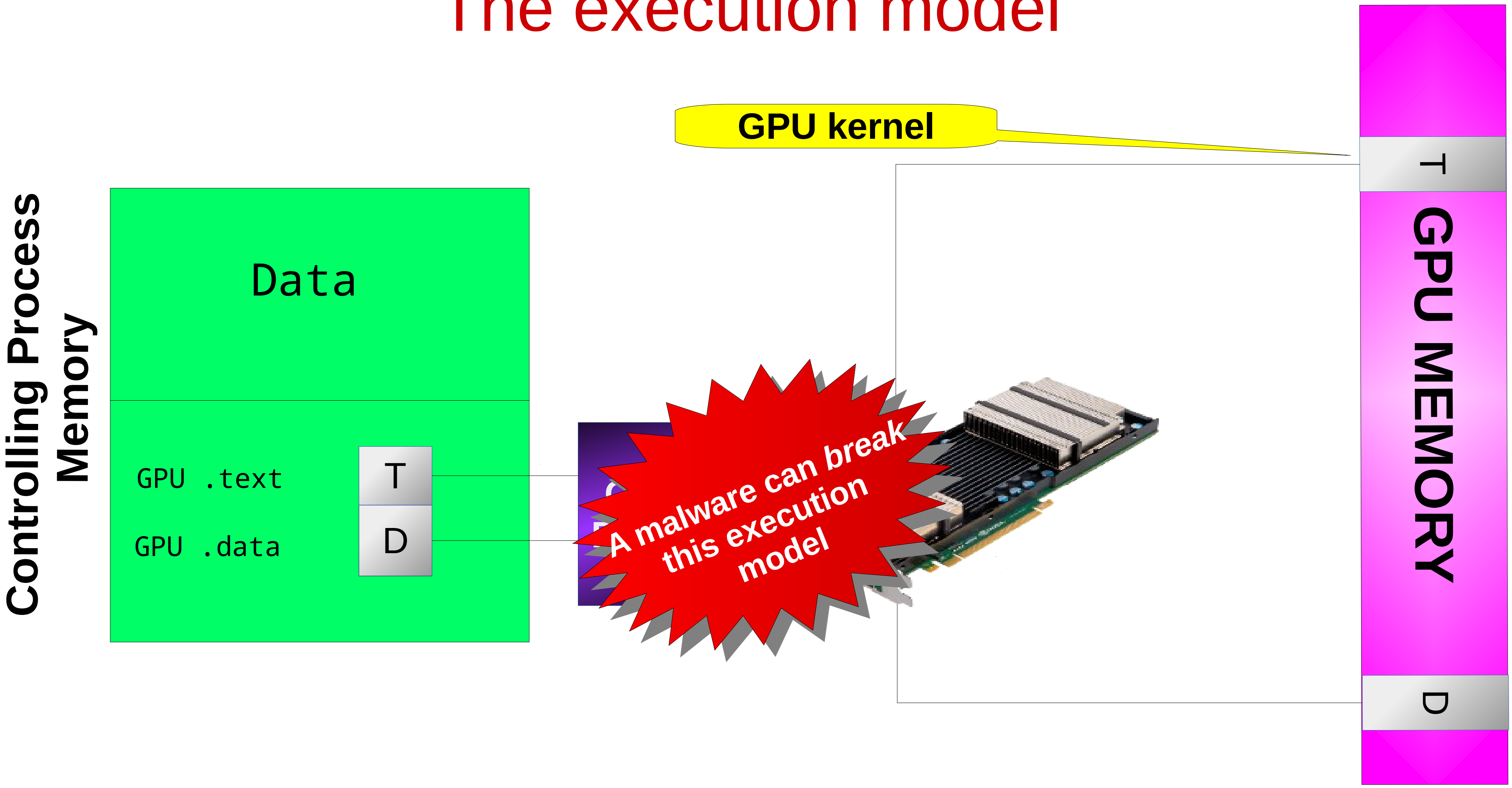
Process list
(e.g. `struct task_struct`)

Context list
(e.g. `struct i915_hw_context`)

Outline

I. ~~Motivation~~
II. ~~Background~~
III. GPU-assisted malware
IV. Case study: Intel Integrated GPUs
V. Conclusion

The execution model



GPU anti-forensic techniques

- We identified four different techniques
  - Unlimited code execution
  - Process-less code execution
  - Context-less code execution
  - Inconsistent Memory Mapping
- Each technique
  - may require different priviledges / knowledge about the driver internals
  - allows the malware to get different level of stealthiness

Unlimited Code Execution

GPUs are non-preemptive:

- If a GPU is doing computation, it cannot do rendering at the same time
- The graphic driver usually enforces a timeout to kill long lasting kernels

This limits a malware activity since it needs a controlling process

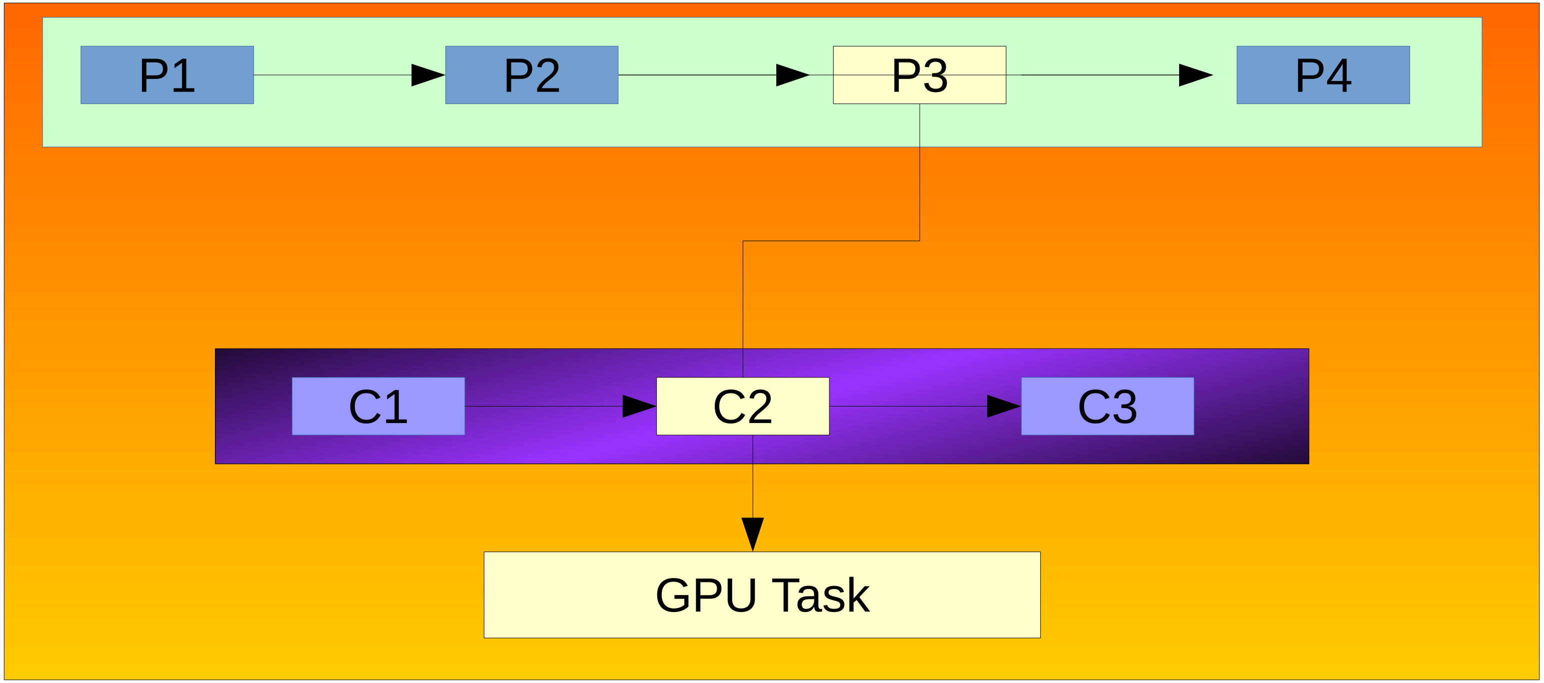
However this limitation can be circumvented so that the malware can get the *Ulimited Code Execution*

Processless execution

In normal condition the graphic driver maintains a link between a task executed in the GPU and its controlling process

The GPU execution model can be broken allowing the presence of a running kernel without any controlling process

Process and Context lists



Process list
(e.g. trask_struct_t)

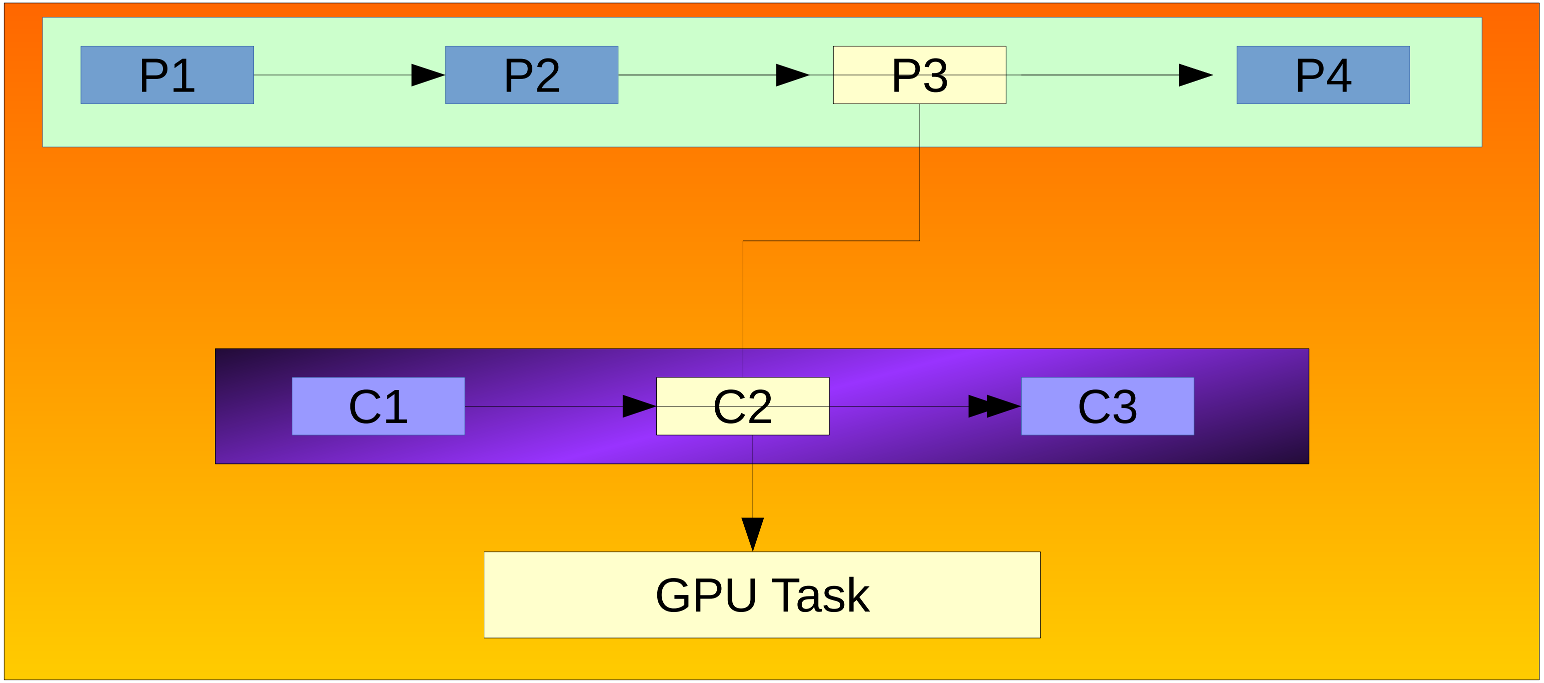
Context list
(e.g. `struct i915_hw_context`)

Contextless execution

The graphic drivers stores information about the task being executed on the GPU

A malware can detach its context from the list in the GPU driver and remove traces about its existence

Process and Context lists



Process list
(e.g.
trask_struct_t)

Context list
(e.g. `struct i915_hw_context`)

Inconsistent Memory mapping

GPU and CPU use different information (i.e. different page tables) to perform virtual to physical address translation
Usually, this pieces of information are synchronized

However, a malware can break this information to hide mapped areas that look suspicious (e.g. the keyboard buffer)

GPU-assisted malware and memory forensic

- A forensic analyst needs to answer a certain number of questions
  - Which processes are using the GPU? (**List processes**)
  - What code is running within the GPU? (**List kernels**)
  - Which part of the host memory is accessed by the GPU? (**List GPU memory maps**)
- **Is the host memory enough to answer to these three questions?**

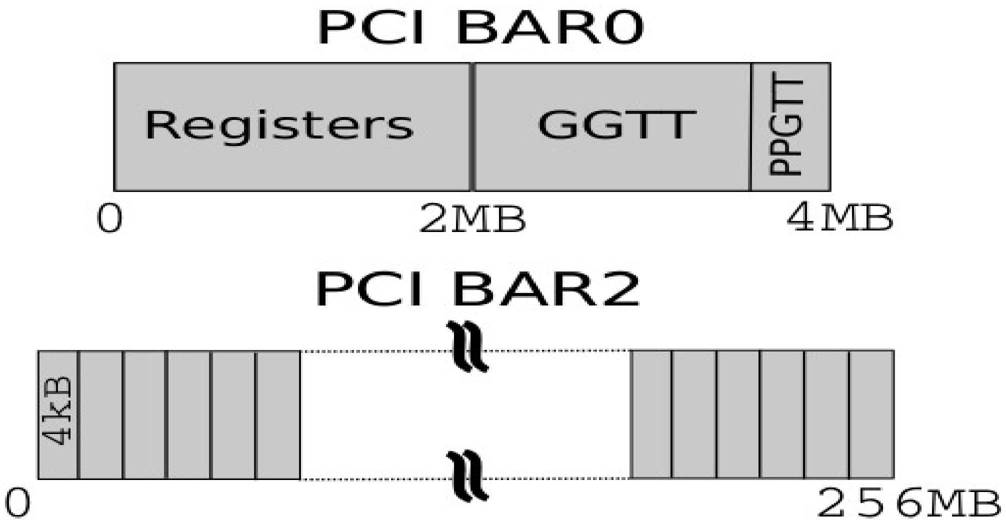
Outline

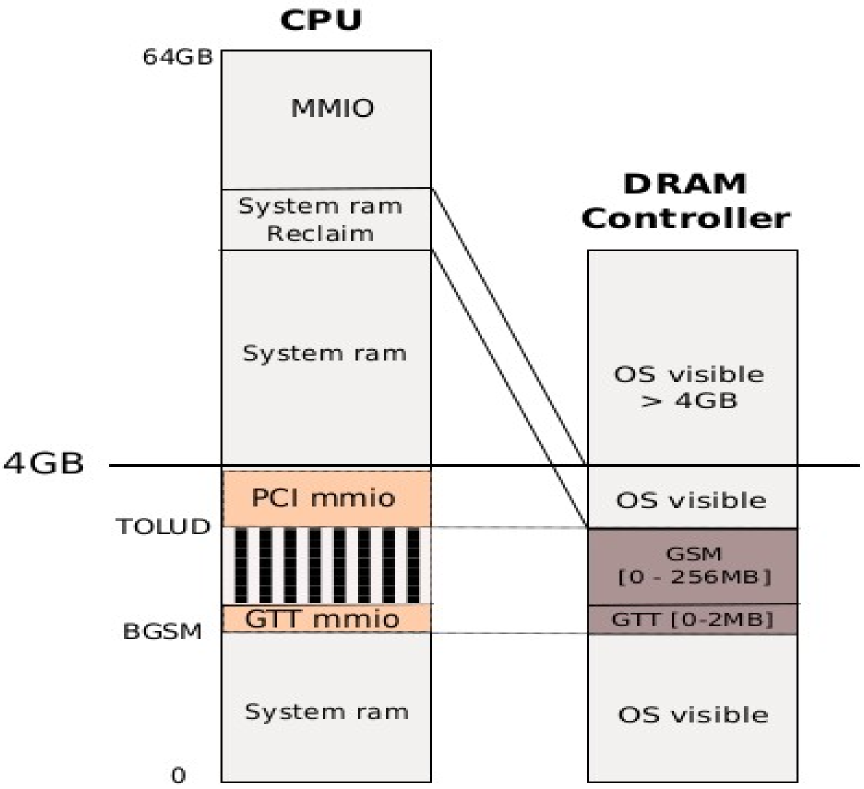
I. ~~Motivation~~
II. ~~Background~~
III. ~~GPU-assisted malware~~
IV. Case study: Intel Integrated GPUs
V. Conclusion

About our case study

- Intel Integrated GPUs of the Haswell processors family
- Linux 3.14
- Direct Rendering Manager (DRM)
  - Graphic Execution Manager (GEM)
    - i915.ko kernel module
- Beignet (OpenCL)

The Address Space Layout on Intel Haswell





PPGTT points to System RAM!

Findings on Intel GPUs

- **Inconsistent Memory Mapping**
  - Change virt to phys mapping inside the PPGTT (it also breaks the W^X bit)
- **Process-less execution**
  - Kill the controlling process after the GPU kernel submission
- **Context-less execution**
  - DKOM attack on the driver data structures (after the GPU kernel execution):
    - Access the struct `drm_i915_private` and gets the `context_list` pointer
    - Call `i915_gem_context_unreference()` on our `i915_hw_context`
- **Unlimited Code Execution**
  - disable the hangheck through the sysfs, at the path
    `/sys/module/i915/parameters/enable hangcheck`

Artifacts of Intel GPUs

- `Hangcheck flag status`
- `struct drm_i915_private`
  - List of contexts
  - List of buffer objects
  - List of process using the GPU
- `PCI BAR0`
  - Register file
  - GTT
  - PPGTT

A plugin for Volatility will be released soon

Need to modify the MA

Host memory limitations

AF Technique	Malware Requirem.	List Process	List Kernels	Memory map
None	U	OS	Driver	OS
Unlimited exec	S	OS	Driver	OS
Process-less	S	N/A	Driver	Driver
Inconsistent	K	OS	Driver	N/A
Context-less	K	N/A	N/A	N/A

Outline

I. ~~Motivation~~
II. ~~Background~~
III. ~~GPU-assisted malware~~
IV. ~~Case study: Intel Integrated GPUs~~
V. Conclusion

Conclusions

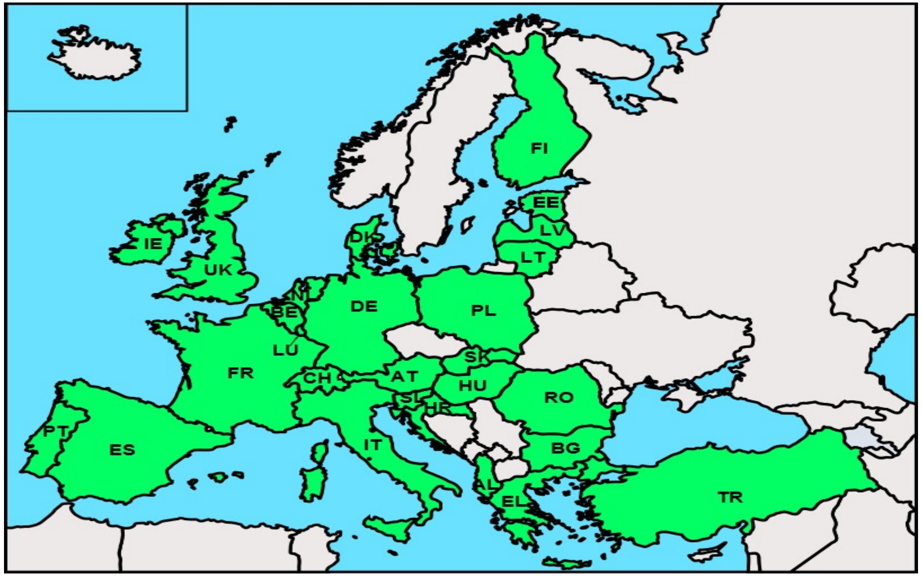
- GPU-assisted malware can become a serious threat in the near future
  - First PoC published (e.g. Demon)
- Lack of:
  - analysis tools
  - Memory acquisition tools supporting this threat
- OS, vendor and family seriously affects the analysis

Acknowledgment

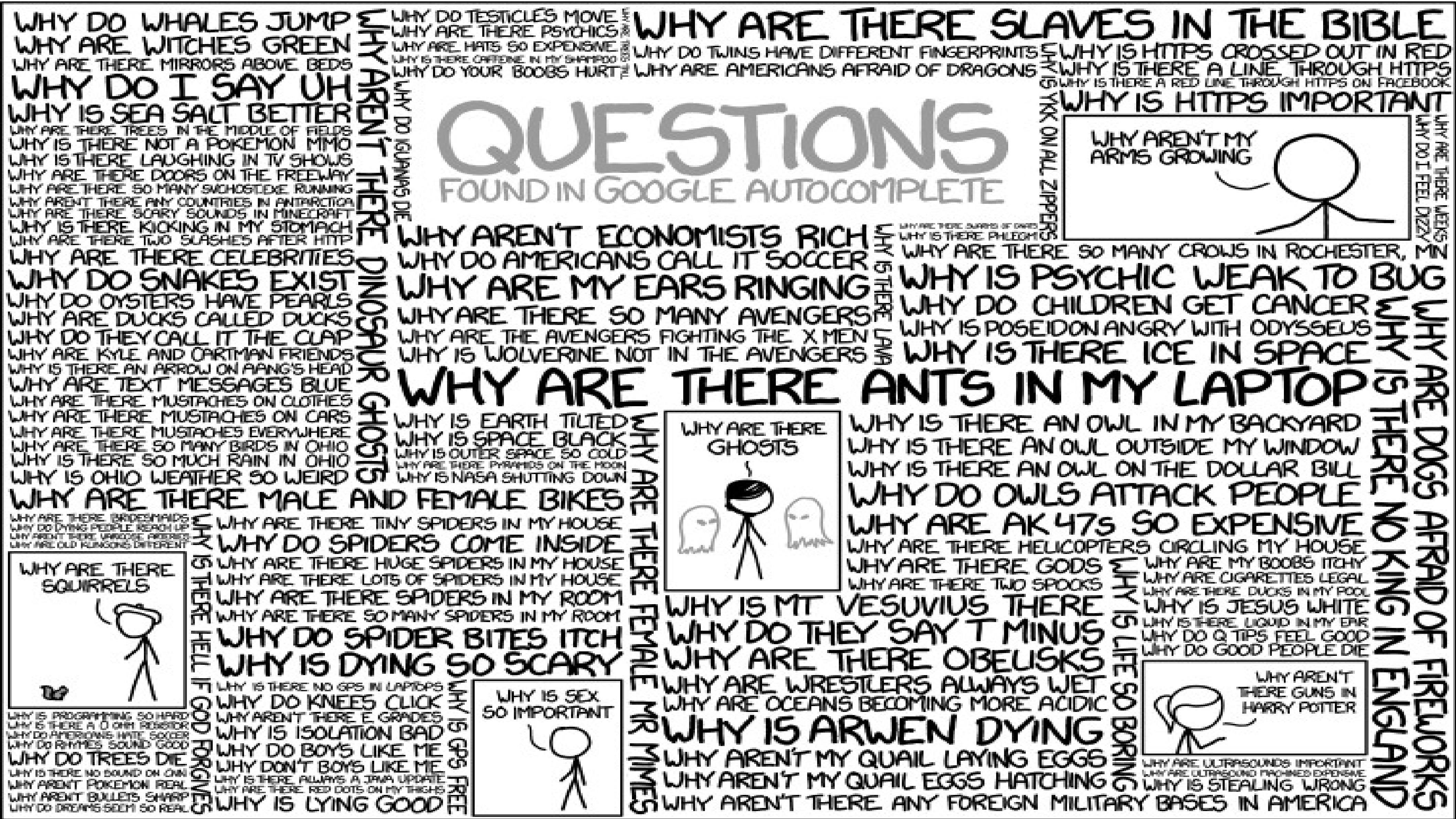
European Antitrust Forensic IT Tools (EAFIT)

AGCM AUTORITÀ GARANTE DELLA CONCORRENZA E DEL MERCATO

ROMA TRE UNIVERSITÀ DEGLI STUDI



This work partially supported by the ***European Antitrust Forensic IT Tools*** *project (rif. HOME/2012/ISEC/FP/C2/4000003977) funded by the Prevention of and Fight against Crime Programme of the European Union European Commission*


QUESTIONS
FOUND IN GOOGLE AUTOCOMPLETE
WHY DO WHALES JUMP
WHY ARE WITCHES GREEN
WHY ARE THERE MIRRORS ABOVE BEDS
WHY DO I SAY UH
WHY IS SEA SALT BETTER
WHY ARE THERE TREES IN THE MIDDLE OF FIELDS
WHY IS THERE NOT A POKEMON MMO
WHY IS THERE LAUGHING IN TV SHOWS
WHY ARE THERE DOORS ON THE FREEWAY
WHY ARE THERE SO MANY SVCHOST.EXE RUNNING
WHY AREN'T THERE ANY COUNTRIES IN ANTARCTICA
WHY ARE THERE SCARY SOUNDS IN MINECRAFT
WHY IS THERE KICKING IN MY STOMACH
WHY ARE THERE TWO SLASHES AFTER HTTP
WHY ARE THERE CELEBRITIES
WHY DO SNAKES EXIST
WHY DO OYSTERS HAVE PEARLS
WHY ARE DUCKS CALLED DUCKS
WHY DO THEY CALL IT THE CLAP
WHY ARE KYLE AND CARTMAN FRIENDS
WHY IS THERE AN ARROW ON AANG'S HEAD
WHY ARE TEXT MESSAGES BLUE
WHY ARE THERE MUSTACHES ON CLOTHES
WHY ARE THERE MUSTACHES ON CARS
WHY ARE THERE MUSTACHES EVERYWHERE
WHY ARE THERE SO MANY BIRDS IN OHIO
WHY IS THERE SO MUCH RAIN IN OHIO
WHY IS OHIO WEATHER SO WEIRD
WHY AREN'T THERE DINOSAUR GHOSTS
WHY DO IGUANAS DIE
WHY DO TESTICLES MOVE
WHY ARE THERE PSYCHICS
WHY ARE HATS SO EXPENSIVE
WHY IS THERE CAFFEINE IN MY SHAMPOO
WHY DO YOUR BOOBS HURT
WHY ARE THERE SLAVES IN THE BIBLE
WHY DO TWINS HAVE DIFFERENT FINGERPRINTS
WHY ARE AMERICANS AFRAID OF DRAGONS
WHY IS YKK ON ALL ZIPPERS
WHY IS HTTPS CROSSED OUT IN RED
WHY IS THERE A LINE THROUGH HTTPS
WHY IS THERE A RED LINE THROUGH HTTPS ON FACEBOOK
WHY IS HTTPS IMPORTANT
WHY AREN'T MY ARMS GROWING
WHY ARE THERE WEEKS
WHY DO I FEEL DIZZY
WHY IS THERE PHLEGM
WHY AREN'T ECONOMISTS RICH
WHY DO AMERICANS CALL IT SOCCER
WHY ARE MY EARS RINGING
WHY ARE THERE SO MANY AVENGERS
WHY ARE THE AVENGERS FIGHTING THE X MEN
WHY IS WOLVERINE NOT IN THE AVENGERS
WHY IS THERE LAVA
WHY ARE THERE SO MANY CROWS IN ROCHESTER, MN
WHY IS PSYCHIC WEAK TO BUG
WHY DO CHILDREN GET CANCER
WHY IS POSEIDON ANGRY WITH ODYSSEUS
WHY IS THERE ICE IN SPACE
WHY ARE THERE ANTS IN MY LAPTOP
WHY IS THERE NO KING IN ENGLAND
WHY ARE DOGS AFRAID OF FIREWORKS
WHY IS EARTH TILTED
WHY IS SPACE BLACK
WHY IS OUTER SPACE SO COLD
WHY ARE THERE PYRAMIDS ON THE MOON
WHY IS NASA SHUTTING DOWN
WHY ARE THERE FEMALE MR MIMES
WHY ARE THERE GHOSTS
WHY IS THERE AN OWL IN MY BACKYARD
WHY IS THERE AN OWL OUTSIDE MY WINDOW
WHY IS THERE AN OWL ON THE DOLLAR BILL
WHY DO OWLS ATTACK PEOPLE
WHY ARE AK 47s SO EXPENSIVE
WHY ARE THERE HELICOPTERS CIRCLING MY HOUSE
WHY ARE THERE GODS
WHY ARE THERE TWO SPOCKS
WHY IS LIFE SO BORING
WHY ARE MY BOOBS ITCHY
WHY ARE CIGARETTES LEGAL
WHY ARE THERE DUCKS IN MY POOL
WHY IS JESUS WHITE
WHY IS THERE LIQUID IN MY EAR
WHY DO Q TIPS FEEL GOOD
WHY DO GOOD PEOPLE DIE
WHY ARE THERE MALE AND FEMALE BIKES
WHY ARE THERE BRIDESMAIDS
WHY DO DYING PEOPLE REACH UP
WHY AREN'T THERE VARICOSE ARTERIES
WHY ARE THERE SQUIRRELS
WHY IS THERE HELL IF GOD FORGIVES
WHY ARE THERE TINY SPIDERS IN MY HOUSE
WHY DO SPIDERS COME INSIDE
WHY ARE THERE HUGE SPIDERS IN MY HOUSE
WHY ARE THERE LOTS OF SPIDERS IN MY HOUSE
WHY ARE THERE SPIDERS IN MY ROOM
WHY ARE THERE SO MANY SPIDERS IN MY ROOM
WHY DO SPIDER BITES ITCH
WHY IS DYING SO SCARY
WHY IS THERE NO GPS IN LAPTOPS
WHY DO KNEES CLICK
WHY AREN'T THERE E GRADES
WHY IS ISOLATION BAD
WHY DO BOYS LIKE ME
WHY DON'T BOYS LIKE ME
WHY IS THERE ALWAYS A JAVA UPDATE
WHY ARE THERE RED DOTS ON MY THIGHS
WHY IS LYING GOOD
WHY IS GPS FREE
WHY IS SEX SO IMPORTANT
WHY IS PROGRAMMING SO HARD
WHY IS THERE A 0 OHM RESISTOR
WHY DO AMERICANS HATE SOCCER
WHY DO RHYMES SOUND GOOD
WHY DO TREES DIE
WHY IS THERE NO SOUND ON CNN
WHY AREN'T POKEMON REAL
WHY AREN'T BULLETS SHARP
WHY DO DREAMS SEEM SO REAL
WHY IS MT VESUVIUS THERE
WHY DO THEY SAY T MINUS
WHY ARE THERE OBELISKS
WHY ARE WRESTLERS ALWAYS WET
WHY ARE OCEANS BECOMING MORE ACIDIC
WHY IS ARWEN DYING
WHY AREN'T MY QUAIL LAYING EGGS
WHY AREN'T MY QUAIL EGGS HATCHING
WHY AREN'T THERE ANY FOREIGN MILITARY BASES IN AMERICA
WHY AREN'T THERE GUNS IN HARRY POTTER
WHY ARE ULTRASOUNDS IMPORTANT
WHY ARE ULTRASOUND MACHINES EXPENSIVE
WHY IS STEALING WRONG