CITS5503 Cloud Computing 2023 Introduction

Dr Zhi Zhang

- Prior to Joining UWA
  - Ph.D. at UNSW
  - Research Scientist in Cyber Security at CSIRO, Data61
- Research Interests
  - Virtualization Security and Operating System Security
  - https://zhangzhics.github.io

Three main cloud providers

Three main virtual machine monitors (VMM)

Hyper-V
- Closed-source
- Microsoft kernel module

Xen and KVM
- Open-source
- Build from scratch

KVM
- Open-source
- Linux kernel module

DRAFT XSA 78 - Insufficient TLB flushing in VT-d (iommu) code

Xen.org security team <security@xen.org>
Wed 20/11/2013 16:37

To: xen-devel@lists.xenproject.org <xen-devel@lists.xenproject.org>; yqcheng.2008@phdis.smu.edu.sg <yqcheng.2008@phdis.smu.edu.sg>; zhangzhi2022@hotmail.com <zhangzhi2022@hotmail.com>; junqing@pku.edu.cn <junqing@pku.edu.cn>
Cc: Xen.org security team <security@xen.org>

1 attachments (1 KB)
xsa78.patch;

***** DRAFT DRAFT DRAFT *****

Xen Security Advisory XSA-78

Insufficient TLB flushing in VT-d (iommu) code

ISSUE DESCRIPTION
==========

An inverted boolean parameter resulted in TLB flushes not happening upon clearing of a present translation table entry. Retaining stale TLB entries could allow guests access to memory that ought to have been revoked, or grant greater access than intended.

IMPACT
======

Malicious guest administrators might be able to cause host-wide denial of service, or escalate their privilege to that of the host.

Re: [BUG] Mapping Assignment Conflict in Dom0 Page Table

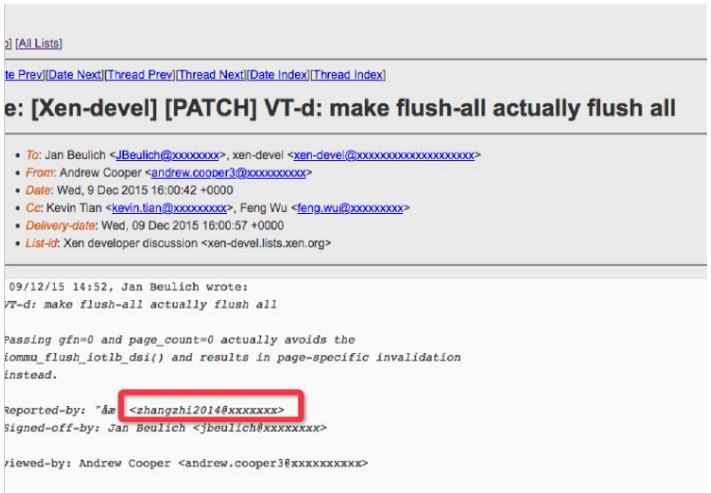
Tim Deegan <tim@xen.org>
Thu 02/01/2014 14:42

To: CHENG Yueqiang <yqcheng.2008@phdis.smu.edu.sg>
Cc: security@xenproject.org <security@xenproject.org>; zhangzhi2022@hotmail.com <zhangzhi2022@hotmail.com>; junqing@pku.edu.cn <junqing@pku.edu.cn>

Hi,

Thanks very much for the report!

At 12:26 +0000 on 02 Jan (1388661998), CHENG Yueqiang wrote:
> Potential Bug Descriptions
> In versions of xen 4.2.x, we find that there exists an assignment conflict between function alloc_l2_table and function create_pae_xen_mappings.
> Attackers may be able to use this potential bug to compromise Xen.
> (Note: arch of the PV guest OS is i386 with PAE enabled.)
>



[All Lists]

[Date Prev][Date Next][Thread Prev][Thread Next][Date Index][Thread Index]

e: [Xen-devel] [PATCH] VT-d: make flush-all actually flush all

- *To*: Jan Beulich <JBeulich@xxxxxxxx>, xen-devel <xen-devel@xxxxxxxxxxxxxxxxxxx>
- *From*: Andrew Cooper <andrew.cooper3@xxxxxxxxx>
- *Date*: Wed, 9 Dec 2015 16:00:42 +0000
- *Cc*: Kevin Tian <kevin.tian@xxxxxxxxx>, Feng Wu <feng.wu@xxxxxxxxx>
- *Delivery-date*: Wed, 09 Dec 2015 16:00:57 +0000
- *List-id*: Xen developer discussion <xen-devel.lists.xen.org>

09/12/15 14:52, Jan Beulich wrote:
VT-d: make flush-all actually flush all

Passing gfn=0 and page_count=0 actually avoids the
iommu_flush_iotlb_dsi() and results in page-specific invalidation
instead.

Reported-by: "åæ <zhangzhi2014@xxxxxxx>
Signed-off-by: Jan Beulich <jbeulich@xxxxxxxx>

Reviewed-by: Andrew Cooper <andrew.cooper3@xxxxxxxxxx>

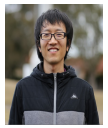
Pre-Requisites and Target Audience

- There will be some coding in this unit and 12 points of programming-based units are required.
- Most students enrolled in the unit are from MIT and should have some computer-science background.

To Get Started

- People
- Emergency
- Items of assessment
- Topics
- Ethics
- Online resources
- FAQs
- What is Cloud Computing?
- Learning outcomes

People



Zhi Zhang
Unit coordinator
Room G.10
zhi.zhang@uwa.edu.au

Hass
School operations team
Room: Main reception
schoolops-pmc@uwa.edu.au

Jichunyang Li
Lab facilitator
jichunyang.li@uwa.edu.au

Abdullah Alelyani
Lab facilitator
abdullah.alelyani@uwa.edu.au

Emergency

- General emergency: call campus security at 6488 2222
- In super emergency: call emergency at 000

- For more details, please have a read through our emergency procedure for various potential incidents
  - http://www.safety.uwa.edu.au/incidents-injuries-emergency/procedures

- For more student services:
  - https://www.uwa.edu.au/students/Support-services
  - UniAccess: https://www.uwa.edu.au/students/Support-services/Disability-and-accessibility (send me your Uniaccess letters ☺)

Assessments

- Labs → 20 %
- Mid-sem Test → 30 %
- Final Exam → 50 %

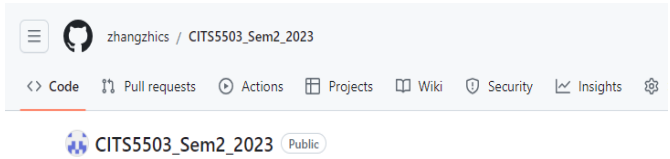
Lectures

- For lectures, they will be recorded and uploaded into LMS.
  - Lectures are about different aspects of cloud computing with exam-style questions included.

Labs start in week 2

- Lab materials
- Lab location
- Lab computer
- Lab assessment
- Lab due dates
- Lab help
- Lab setup

Lab materials

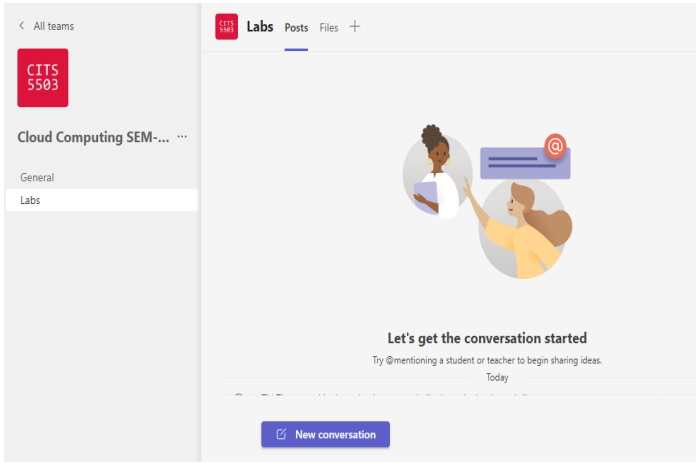


https://github.com/zhangzhics/CITS5503_Sem2_2023

Lab Location

- Labs
  - Labs are in MATH computer lab (Net A and D) and South Civil Computer Room B
  - Check your timetable for your lab allocation
  - You can go to another scheduled lab IF there is a space (normally there is)

MS Teams



Lab Computer

- The labs are related to docker, VirtualBox, Ubuntu OS, etc.
- As docker is NOT available on UWA lab machines, it must be run on your laptops
- If you do not have a laptop that is capable of running the labs, you can arrange to borrow one: https://uwacyber.gitbook.io/cits1003/cits1003-labs/introduction-to-labs
- Else – invest in a decent laptop – it will make a big difference to your University life.
- If none of these options are available to you, please come and chat with me.

Lab Assessment

- Labs are worth 20% of the unit grade (i.e., 20 points in total).
- 9 labs in total: Each lab in labs 1-7 is worth of 2 points and each lab in labs 8-9 is worth of 3 points.
- One lab for each study week Except Week 1,5 and 12.

- Note: Please terminate your AWS (Amazon Web Services) virtual machines after completing a lab.

Lab Assessment

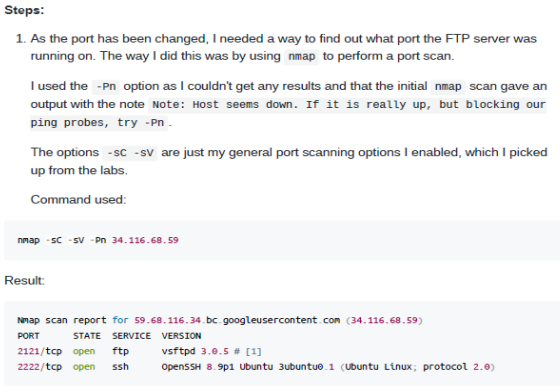
- For every lab, prepare a lab report.
- For each lab report,
  - ➢You should follow all steps in the github (https://github.com/zhangzhics/CITS5503_Sem2_2023)
  - ➢You should include screenshots showing the output for every command line instruction that you execute in the terminal and any other relevant screenshots that demonstrate you followed the steps.
  - ➢You should include your own descriptions about the screenshots.
  - ➢You should include scripts with comments that you create and the corresponding output you get when executed.

Lab Assessment

- Every lab report is marked as follows:
  - A structured description (15%). This is to make sure a report's readability good. We don't provide any template. Instead, you are encouraged to use a markdown editor to organize your reports.
  - A clear step-by-step with detailed descriptions (85%). In each step, screenshots and their descriptions are needed. By doing so, our markers can follow the steps as described to get the answers.

Lab Assessment

- Every lab report is marked as follows:
  - A structured description (15%).
  - A clear step-by-step with detailed descriptions (85%).



Steps:

1. As the port has been changed, I needed a way to find out what port the FTP server was running on. The way I did this was by using `nmap` to perform a port scan.

   I used the `-Pn` option as I couldn't get any results and that the initial `nmap` scan gave an output with the note `Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn`.

   The options `-sC -sV` are just my general port scanning options I enabled, which I picked up from the labs.

   Command used:

```
nmap -sC -sV -Pn 34.116.68.59
```

Result:

```
Nmap scan report for 59.68.116.34.bc.googleusercontent.com (34.116.68.59)
PORT     STATE  SERVICE  VERSION
2121/tcp  open   ftp      vsftpd 3.0.5 # [1]
2222/tcp  open   ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
```

Lab Due Dates

- For labs 1-4, due date: 5pm 1 September (week 6)
  - Report name: studentid_firstname_labs1_4
- For labs 5-9, due date: 5pm 20 October (week 12)
  - Report name: studentid_firstname_labs5_9
- Again, no labs on Week 1,5 and 12.
- Report submissions are via LMS (Similarity detection will be applied)
- The submission must be a single PDF file - all other submissions will be IGNORED. Please note that you can submit multiple times before the due date and only the latest submission will be marked.
- Late submission is allowed but penalty will be applied: a penalty of 5% of the marks allocated for labs1-4 or labs5-9 is deducted per day for the first 7 days after which the submission is not accepted. Each 24-hour block is recorded from the time the assignment is due.

Lab Help

- For labs, one facilitator hosts one lab session
  - Please attend scheduled lab sessions for help.
  - No lab help **outside** the scheduled lab time.

Lab Setup

- Virtual Machine Manager: Virtualbox or VMware
- Setup VM and install Ubuntu

Other Assessments

- Mid-semester test is scheduled in Week 6.
  - Mid-semester test is worth 30% of assessment (more details later)
- Final Exam: 50% of final assessment
  - Exam overview will be done in week 11 or 12.

Enquiries

- Office hours
  - Maybe Friday 12 – 2pm (F2F and virtual) -> this is just an arbitrary slot
  - Other times can be arranged too (send an email)

- Lab Enquiries
  - Ask on Teams (but remember not to share answers)
  - Ping lab facilitators (you can contact any one of them)!
  - If all fails, email me

Misconduct

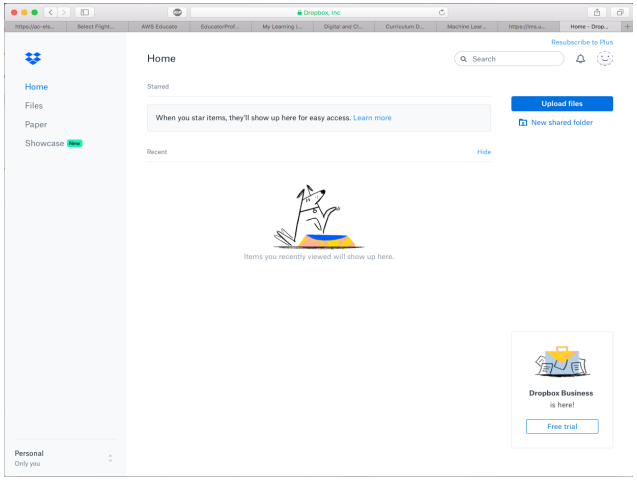
- Please do not cheat on any of the assessment items.
- Don't copy your friend's code/answers/report.
- Don't share your code with your friends
  - Only share ideas

- Consequences are dire!

What is cloud computing?

http://www.dilbert.com/fast/2013-06-29/

Cloud Services



Formal definition

- According to NIST (USA's National Institute of Standards and Technology):

  Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., processors, networks, storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

Formal definition

- According to NIST (USA's National Institute of Standards and Technology):

  Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., processors, networks, storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Essential characteristics/benefits:
  - On-demand self service
    - Cloud providers allows us to provision computing resources, such as virtual machines, without interacting with them.
  - Broad network access
    - cloud services are accessible over a network in various ways.

Formal definition

- According to NIST (USA's National Institute of Standards and Technology):

  Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., processors, networks, storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Essential characteristics/benefits:
  - On-demand self service
  - Broad network access
  - Resource pooling
    - Cloud providers consolidate and share computing resources among many users.
  - Rapid elasticity
    - Cloud providers enables the quick and automatic scaling of underlying hardware resources based on workload demands

Formal definition

- According to NIST (USA's National Institute of Standards and Technology):

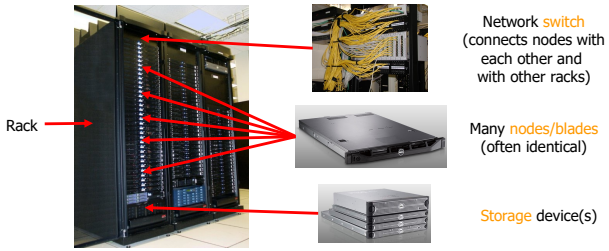
  Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., processors, networks, storage) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

- Essential characteristics/benefits:
  - On-demand self service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service
    - Cloud providers allow users to pay as they go

Motivating Cloud Computing

- What if one computer is not enough?
  - Buy a better (server-class) computer
- What if the best server is not enough?
  - Buy many servers

Cluster



- Characteristics of a cluster:
  - Many similar machines with close interconnection
  - Special and standardized hardware (racks, blades, etc)

Power and cooling

- Clusters need lots of power
  - Most of power is converted into heat
- Large clusters need massive cooling

Scaling up

PC Server Cluster Data center

- What if a cluster is not enough?
  - Buy many clusters

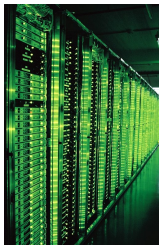
Data center

Cooling plant

Data centers (size of a football field)

Google data center in The Dalles, Oregon

What's inside a data center?



Source: 1&1

- Hundreds or thousands of racks

What's inside a data center?


Source: 1&1

- Massive networking

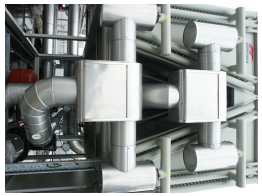
What's inside a data center?



Source: 1&1

- Lots of power supplies

What's inside a data center?




Source: 1&1

- Massive cooling

Scaling up



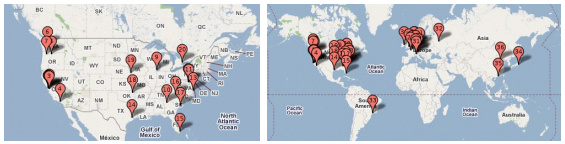


PC Server Cluster Data center Network of data centers

- What if a data center is not big enough?
  - Build many data centers

Global distribution

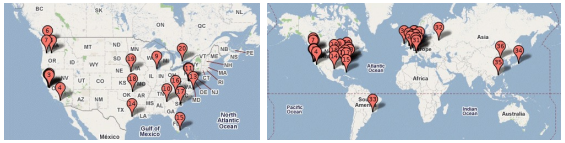
Google data centers



- Data centers are globally distributed and networked
- Why do we need to distribute the data centers globally?

Global distribution

Google data center in The Dalles, Oregon



- Data centers are often globally distributed and networked
- Why do we need to distribute the data centers globally?
  - Reduced Latency
    - We can bring our cloud services closer to users.
  - Disaster Recovery
    - When a data center goes down, other data centers can replicate the data.
  - Regional Markets
    - We can deliver our cloud services that are optimized for specific regional markets.
  - …

Data center has enabled cloud computing

- Big tech companies use existing data centers to provide cloud computing

- Benefits:
  - Economies of scale
    - Cheaper to run big data centers than many small ones
  - Statistical resource multiplexing
    - High utilization of hardware resources
  - No up-front commitment
    - No investment in data centers, enabling pay-as-you-go
  - Scalability
    - Thousands of servers available on demand
    - Add more within seconds

Other terms

- Utility computing
  - Services being provided by a cloud
  - Focuses on the business model (pay-as-you-go), similar to classical utility companies

- The Web
  - The Internet's information sharing model
  - Some web services run on clouds, but not all

- The Internet
  - A network of networks.
  - Used by the web; connects (most) clouds to their customers

Cloud applications

- Application hosting
- Backup and Storage
- Content delivery
- E-commerce
- High-performance computing
- Media hosting
- On-demand workforce
- Search engines
- Web hosting
- …

Some Examples

- DreamWorks applies the Cerelink cloud to render animation movies

- CERN leverages a "science cloud" to process experimental data

- Virgin atlantic hosts their travel portal on Amazon AWS

Practice Questions

- Some questions in mid-semester test are picked from the link below:
  - github.com/zhangzhics/CITS5503_Sem2_2023/blob/master/assignments.md
- Some practice questions are also picked from the link.
  - Answers to practice questions will be discussed in the live lecture.
  - Answers to other questions in the link need your own work.

Practice Questions

- [6 marks] Q1: The evolution of Cloud Computing has been compared to the evolution of electricity supply as a utility. Describe 3 specific problems that Cloud Computing solves as compared to businesses running their own data centers..

- [2 marks] **Operational expenses:** Cloud computing enables businesses to apply a subscription policy without investing in building and maintaining their own data centers.
- [2 marks] **Scalability:** Cloud computing enables on-demand computing resources by providing virtualized computing resources.
- [2 marks] **Resource utilization:** Cloud computing provides multi-tenant environments by allocating resources efficiently for different users, e.g., some tasks are computing intensive while some other are memory intensive.

Practice Questions

- [6 marks] Q2: An established financial company is about to launch their new banking application. Give 3 reasons why the company should use their own data center rather than cloud computing.

- [2 marks] **Data Security**: Financial institutions must ensure CIA of user data security. By hosting their application in their own data center, the company can better protect their data security.
- [2 marks] **Data Sovereignty:** For international financial institutions, data sovereignty is critical because user data will be stored and processed in compliance with local laws and regulations.
- [2 marks] **Optimized Performance:** With their own data center, the company can have consistent performance for their application. Besides, they can fine-tune the infrastructure to optimize the application's performance.

Learning Outcomes

Understandings

- Understand cloud services, their motivation, design and implementation
- Understand the basics of virtualization of hardware, networks and security
- Understand cloud-based web architectures and their applications
- Understand how to achieve scalability and security in a cloud

Hands-on skills

- Use DevOps to deploy and manage the creation and update of software environments
- Use cloud services to carry out specific use cases such as machine learning

Copyright notice