Technology Perspective: Is Green IT a Threat to IT Security?

Dimitrios Frangiskatos, Mona Ghassemian, and Diane Gan

School of Computing and Mathematic Sciences, University of Greenwich, UK

Abstract. Industries are pushed by the regulations to reduce the CO2 footprint of their production lines. According to the latest statistics 3% of the CO2 footprint is generated by the IT industry. Currently a high percentage of the information being accessed by the users is produced and managed centrally. With the growth of data generation by users, e.g. social networking and YouTube websites, the storing and managing of the data will demand more energy on the networks.

One of the solutions to reduce the energy consumption in ICT is introduced by virtualisation technology. While virtualisation can help to reduce the energy consumption, it has introduced other complexities to the environment, such as scalability, resource management, security and management.

This paper focuses on the security issues created by the use of virtualisation technology which is being promoted to make computing Green. We also aim to highlight the system vulnerabilities which are a direct result of pushing computing to become greener by using virtualisation technology. We discuss the research challenges and directions needed to be further investigated in this field.

1 Introduction

Lately there is a lot of discussion around the reduction of greenhouse gasses and environmental and energy consumption issues. New legislation to regulate businesses' environmental impact has been introduced. The Waste Electrical and Electronic Equipment (WEEE), the restricted use of hazardous substances (RoHS) and the battery directive, have been adopted by the EU in an attempt to reduce the risk presented to the environment and human health by hazardous materials when incinerated or put into landfills. Retailers are trying to reduce excessive packaging, the air-freighting of food long distances and to providing alternatives to plastic bags. With regards to the latter, some will say that although allegedly these last for hundreds of years, most usually decompose before you get your shopping back home. Well they may be aware that in some places even bottled water was banned [5] to reduce the environmental impact.

It is not a secret that the IT industry, i.e. ICT (Information and Communication Technologies) uses vast amounts of energy to power the systems it uses to provide its services. Google's data centre's energy requirements have attracted the attention of environmentalists after it was claimed that the amount of energy required for two typical searches could boil a kettle [6]. Google's response was that each search takes approximately 0.0003 kWh [7].

D. Weerasinghe (Ed.): ISDF 2009, LNICST 41, pp. 147–154, 2010.

As the concept of green has an impact on the way people think about computing these days, big IT firms (IBM, HP, Sun and Google) are implementing major green schemes and environmentally friendly solutions. Google has embarked in a solar program for its headquarters, which since 2007 has produced 4,427 megawatt-hours [8].

It has been suggested that PC work places are under utilised, with less than 1% of the CPUs being used in any 24 hr period. Since PC hardware is distributed, each runs an OS and numerous applications, which are duplicated many times and each PC consumes electricity. There is also no resource pooling [15].

Having discussed the energy consumption means and the cost for it, there are number of solutions that the IT industry can use to reduce energy costs and protect the environment; i.e., replace paper with digital copies for business processes, adopt service oriented approaches, optimise systems and opt for virtualisation solutions.

Re-using old equipment is also a way to greener IT. Reusing old equipment for less demanding applications, can save up on raw materials (and thus energy) and reduce landfill waste. The rule is however that before donating or recycling used equipment, the hardware must be thoroughly cleansed of all data, not just data protected by privacy and security regulations. In a recent article [11] it was revealed that a security expert discovered that a VPN device bought on EBay automatically connected to a local council's confidential servers. The alternative to this is to use virtualisation.

Virtualisation is widely adapted today as a mainstream technology in IT. Virtualisation works by inserting a thin layer of software directly on the computer hardware

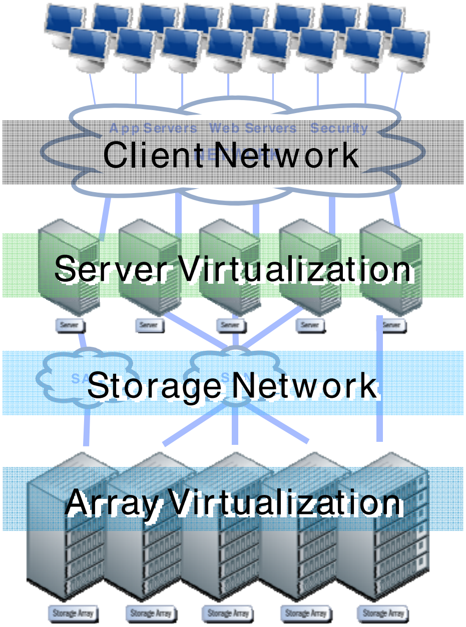

Fig. 1. Virtualisation is everywhere [13]

or on a host operating system. This contains a virtual machine monitor or “hypervisor” that allocates hardware resources dynamically and transparently. Pool common virtual infrastructure resources break the legacy “one application to one server” model with server consolidation, which dramatically improves the efficiency and availability of resources and applications in every organization.

Fewer servers and related IT hardware means reduced physical infrastructure, reduced power and cooling requirements and improved server to admin ratio. However there are voices of concern: can something be overlooked? After all, each VM is another server that an administrator must manage. Security updates must be applied and global configuration changes now need to be propagated to all of these new machines.

Virtualising a single physical computer is just the beginning. The four key elements that can be identified for virtual infrastructures are: clients, storage, servers and networks as depicted in Figure 1.

An automated data centre, built on a virtualisation platform responds to market dynamics faster and more efficiently than ever before. Management of a data centre on a virtual network architecture is a new dimension of research that is discussed and proposed in this work. Beside the flexibility, availability, efficiency and scalability features, a virtual data centre is green. According to VMware statistics [12] their customers typically save 50-70% on overall IT costs by consolidating their resource pools and delivering highly available machines with VMware Infrastructure.

Today’s data centres consume a lot of electricity. A recent report by the Environmental Protection Agency claims data centres in the U.S. consume 4.5 billion kWh annually, 1.5% of the country’s total. Perhaps more importantly, this figure has doubled from 2000 to 2006, and is likely to double again in the next few years. This trend is affecting data centres around the world and is likely to continue, given how central computing is to today’s businesses and current lifestyles.

A virtualisation layer takes care of resource allocation from different data centre locations and all specifics when service instances are allocated in a particular data centre. Virtualised data centres provide a consistent operating environment spanning multiple physical data centre locations for the whole family of service instances [3].

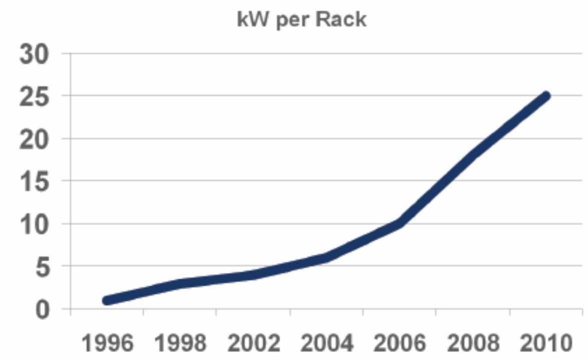

Fig. 2. Rising Energy Consumption in the Data Centre [1]

2 Research Challenges

While virtualisation technology has developed quite a long way from the basic elements in IT (machines, storage and networks), new research challenges have been turning into an increasing problem.

Most of the existing research work related to network virtualisation is discussed in [4], namely, interfacing, signalling and bootstrapping, resource and topology discovery, resource allocation, admission control and usage, virtual nodes and virtual links, naming and addressing, mobility management, monitoring, configuring and failure handling, security and privacy, interoperability issues and finally economics. Virtualisation is about sharing across IT domains, and that is often the problem. In this work we focus on the problems of security and management of virtualisation.

A. Virtual Network Security and Threats

In this section we investigate additional complexities and security threats as a result of using virtualisation.

Virtualisation is seen by many as a way of achieving green security. A growing number of security professionals are also considering the cost-cutting benefits of green security. Companies who have gone over to green security have found that having a smaller carbon footprint may not necessarily be a hindrance to maintaining their defences. Shrinking the number of boxes reduces costs and at the same time saves the planet by cutting the company's carbon footprint. The money saved can be used to spend on virtual security devices. There are currently a number of these devices on the market which reduce power consumption without compromising security [18].

Some organisations use virtualisation as a security substitute. Consolidating the data centre using virtualisation saves power, but integrating it to existing systems introduces many significant security challenges. Deploying virtual servers means that the physical cables that connect the original servers are no longer present. If security gateways were present between these servers then they no longer exist in the virtual world. If one virtual server in a data centre is compromised this could potentially put the rest at risk. Although virtualisation vendors have used the fact that their products will protect your data from malware as one of the selling points for their products, physical separation of systems should be used instead. As we know, for a number of years developers have been writing code for applications, operating systems and hardware that cannot be assumed to be bug free. It is safe to assume that virtualised solutions will have similar security issues. It is just a matter of time before they are discovered. VMware customers were recently prevented from logging onto their virtual servers as a bug distributed in a software update effectively stopped systems from powering up [9]. Other critical vulnerabilities which allow a host operating system to run code on the host have been also identified [10]. To date there have been a number of patches issued by VMware, for software flaws. The biggest threat is not to the virtual servers themselves, but to the "hypervisor", with denial of service attacks being perceived as the main threat. [14]

<u>*Security issues with server sprawling*</u>: Server sprawling although good for the environment can be responsible for virtualised solutions that are inappropriate for a

number of reasons. The problem lies with the fact that servers can be created with the click of a button, without the usual physical constraints. This can lead to reduced efficiency which contradicts one of the key benefits of virtualisation. While the well-meaning administrator may be seeking to achieve objectives such as research or recovery, "extra" copies of VM environment can possibly sit dormant, not receiving the operating system or application patches needed to keep the VM secure. This creates vulnerability should these VMs, which are not up to the security standard, be re-introduced into the production environment [17].

Application performance on top of VM: Running virtual machines on a physical machine requires a lot of hardware resources, and unless properly configured, performance will be noticeably slow. With that in mind, certain parameters of applications running on top of a VM can be overlooked and that can lead to poorly configured applications. Problem diagnosis in VM servers might not be as straightforward to detect as in a non virtualised system.

Tracing of security incidents: With virtualised solutions the insider threat is greater than ever. In the past it wasn't easy for a disgruntled employee to take a server home, compromise it and then take it back to work. Now it is easy for someone to copy a number of virtualised machines on a USB, alter them at home and then copy them back to the company's network the following day.

Encryption standards in VM encryption

A provider may allow multiple customers to administer virtual machines on the same physical host but how well do different virtualisation environments protect or isolate one virtual machine from another? Especially when considering that there is not yet a standard for encrypting VM environments.

"Isolation between coexisting VNs can only provide a certain level of security and privacy through the use of secured tunnels, encryptions and so on; but it does not obviate the prevalent threats, intrusions, and attacks to the physical layer and VNs. In addition to that, security and privacy issues specific to network virtualisation must also be identified and explored. For example, programmability of the network elements can increase vulnerability if secure programming models and interfaces are unavailable. All these issues require close examination to create a realistic NVE."[4]

Network segmentation: Internal virtual network segmentation within a host and between its various VMs is also possible with the virtualisation tools, but this flexibility runs the risk that internal virtual segments cannot be reached from the external network. This could hamper traditional ingress security techniques, such as antivirus updates or operating system updates, or egress security techniques such as monitoring/alerting or log consolidation [17].

B. Virtual Network Management

Unlike the established and distinct roles for managing physical systems, networks and storage, virtualisation is not owned by a specific role. Rather it cuts across the three domains. Virtual elements are often not even considered as managed entities since they do not exist physically and are not inventoried. The Management Information

Base (MIB) is required to be compiled into the virtual management system. Consequently, management practices are often not applied to virtual entities such as change, configuration and release management processes.

Due to the fact that virtual resources, in the end, rely on sharing physical resources, estimating workloads, planning capacity and achieving predictable behaviour is becoming much harder with little evidence or experience from past providing guidance.

Most established management systems are not prepared and are of no help in dealing with virtual elements. One reason is that virtual entities can be created in an ad hoc manner and may only exist for a short time [2]. They also may not be active all the time and rather exist in a saved state which can be resumed at any time to recreate a virtual entity. This leads, in many cases, to the fact that virtual entities cannot be discovered, uniquely identified and registered in configuration and management databases. Hence, they are often unknown to management systems which rely on the information in those databases.

The benefits of virtualisation are undeniable. However, the virtual world residing in that clean and organized physical world can easily become unaggregated, fragmented and unmaintained leading to high management overhead, unpredictable risk of failure and chain effects.

Management software for virtual infrastructures, such as Virtualisation 2.0, is now in its second phase. This places an additional layer of software on the virtual platforms. The various layers of software (applications, protocol layers, OS in VMs and the virtualisation platform) must all work together to provide a business service. [16]

VMs can be cloned with a complete collection of applications installed on top of an operating system. When the duplicate (or more) VM(s) are created, the organisation needs to ensure their licensing agreement with the vendors covers that type of instance [17].

Staff skills must grow to meet the complexity of the more centralized resource allocation duties placed on the administrator of the virtualisation tools. Physical server team members, while competent in networking concepts, are usually placed in a role where they may create multiple virtual switches, VLANs, and maybe deploy a VM with router capabilities. The server team members need a combination of increased training and increased communication with the physical network team as well as the information security team [17].

Cloud computing is one of the fastest growing segments in the IT industry with companies tapping into the cloud to boost their infrastructure resources at a low cost. The idea behind cloud computing is based on multi tenancy and decoupling between specific hardware resources and applications. However there are concerns regarding the security because of the multi tenant feature of the cloud and the fact that there are no standards for security or data privacy. There is a slight reluctance on the part of cloud providers to create standards as there are concerns that cloud computing remains at such an embryonic stage that the imposition of strict standards could do more harm than good. Certain companies try to adapt ISO27001 for use with cloud based applications however that is not a panacea. Experts' advice to companies is to invest in monitoring tools and keep systems updated. At the same time security policies should be thoroughly reviewed and service availability guarantees and penalties should be scrutinised. However, cloud security policies cannot always accommodate an individual company's needs. That creates gaps in the cloud pot of data that can be exploited by attackers. Recent examples include Gmail's service which collapsed in Europe [19] and Saleforce's phishing attack [20].

3 Summary

A significant amount of virtualisation is already implemented in IT industry, e.g. data centres which eliminates hard-wire association, server Consolidation and increase the energy efficiency. For this scenario, a virtualisation solution reduces the energy demands of running a data centre by server consolidation (one device can appear as many) and dynamic management of computer capacity across a pool of servers. However there are further questions remain to be investigated such as the extra added management complexity and security threat for the storage network.

Fundamental concepts of management such as determining the existence and the identification of virtual entities are unresolved. Existing management systems hence remain unaware and incapable of managing virtual entities.

The goals of monitoring and assessment of virtual environments are a continuous process and more ad hoc. Associations of virtual entities to underlying shared resources are also often not represented, making fundamental management tasks such as monitoring problematic. While data can be collected using current monitoring systems, correct interpretation is often not possible because the context of the measurement or probing was not captured, such as the association of virtual entities to underlying physical entities at a given point in time. While a compromised virtual server can easily be replaced with a clean copy, the question remains, how many organisations would be able to identify that there was a problem quickly enough to avert any further problems?

The bottom line is that in today's growing virtual networks, to avoid longer term and more costly issues, it is critical to assess the current state and to implement policies, procedures, and tools to evaluate mitigation of the risks of virtualisation [17].

A solution must be found that can continue to reduce power usage and hence energy costs, while at the same time solving the business needs of organisations. While this paper has possibly raised more questions than it has answered, this is an ongoing work. The security challenges of using virtualisation technology to address the Green challenges of the future cannot be underestimated.

References

[1] How VMware Virtualisation Right-sizes IT Infrastructure to Reduce Power Consumption, VMware White paper

[2] Graupner, S.: Virtualised IT Infrastructures and Their Management. In: Workshop on Virtualised IT Infrastructures and Their Management (October 2008)

[3] Graupner, S., Kotov, V., Trinks, H.: Resource-sharing and service deployment in virtual data centres. In: Proceedings of 22nd International Conference on Distributed Computing Systems, pp. 666–671 (2002)

[4] Mosharaf Kabir Chowdhury, N.M., Boutaba, R.: Network Virtualisation: state of the art and research challenges. IEEE Communications magazine 47(7), 20–26 (2009)

[5] http://enjoybottledwater.org/?p=37

[6] http://technology.timesonline.co.uk/tol/news/tech_and_web/article5489134.ece

[7] http://www.thenakedscientists.com/HTML/content/questions/question/2246/

[8] http://www.google.com/corporate/solarpanels/home

[9] http://www.networkworld.com/news/2008/081208-vmware-bug.html

[10] http://www.securityfocus.com/archive/1/archive/1/502615/100/0/threaded

[11] http://www.pcpro.co.uk/news/227190/council-sells-security-hole-on-ebay.html

[12] VMware website, http://www.vmware.com/pdf/vi3_monitoring_statistics_note.pdf

[13] Mellish, B.: Best Practices in Managing Virtualised Environments. Storage Networking Industry Association (May 2009)

[14] Saran, C.: Virtualisation Presents Security Challenges. Computer Weekly, posted 9, 45 (March 26, 2008)

[15] Virtual Workplace – White Paper (Fijitsu) (March 2008)

[16] Virtualisation 2.0 is all about Manageability – White Paper, http://www.eginnovations.com/whitepaper/Virtualisation2_0.pdf

[17] Hoesing, M.T.: Virtualisation Security Assessment. Information Security Journal: A Global Perspective (January 2009)

[18] Bill Brenner, Cost cutting through Green IT Security: Real or Myth? (June 2008), http://www.csoonline.com/article/print/410513

[19] http://www.theherald.co.uk/news/news/display.var.2491445.0.Google_apologises_to_millions_after_gmail_collapse.php

[20] http://www.computerworlduk.com/management/security/cybercrime/news/index.cfm?newsid=6058