INFORMATION SECURITY TECHNICAL REPORT XXX (2011) 1–8

Available online at www.sciencedirect.com

SciVerse ScienceDirect

www.compseconline.com/publications/prodinf.htm

Information Security Technical Report

Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization

André van Cleeff [a,*], Wolter Pieters [a], Roel Wieringa [a], Frits van Tiel [b]

[a] University of Twente, Enschede, The Netherlands
[b] TUNIX Internet Security, Nijmegen, The Netherlands

ABSTRACT

Virtualization is one of the enabling technologies of cloud computing. It turns once dedicated physical computing resources such as servers into digital resources that can be provisioned on demand. Cloud computing thus tends to replace physical with digital security controls, and cloud security must be understood in this context. In spite of extensive research on new hardware-enabled solutions such as trusted platforms, not enough is known about the actual physical-digital security trade-off in practice. In this paper, we review what is currently known about security aspects of the physical-digital trade-off, and then report on three case studies of private clouds that use virtualization technology, with the purpose of identifying generalizable guidelines for security trade-off analysis. We identify the important security properties of physical and digital resources, analyze how these have been traded off against each other in these cases, and what the resulting security properties were, and we identify limits to virtualization from a security point of view. The case studies show that physical security mechanisms all work through inertness and visibility of physical objects, whereas digital security mechanisms require monitoring and auditing. We conclude with a set of guidelines for trading off physical and digital security risks and mitigations. Finally, we show how our findings can be used to combine physical and digital security in new ways to improve virtualization and therefore also cloud security.

© 2011 Elsevier Ltd. All rights reserved.

1. Introduction

Two trends occur in IT: the first is virtualization, the creation of software layers with the goal of separating higher-level applications from the underlying physical components. The second concerns the creation of cyber-physical systems (CPS), where IT systems are specifically designed to integrate with the physical world, for example smart phones with motion sensors or patient health monitoring systems and household robots.

Both trends cause security problems: CPS can be attacked from both cyberspace and physical space, leading to new classes of attacks, which combine both: cyber-enabled physical attacks and physically-enabled cyber-attacks (DePoy et al., 2006). An example of the former is an attack where the engine controller of a car is remotely controlled (Krogh et al., 2008), causing a full-stop on the highway. Likewise, virtualization also leads to security issues: virtualized systems scale very well, but so do the attacks on these systems, which are no longer hindered by physical barriers.

* Corresponding author.
E-mail addresses: a.vancleeff@utwente.nl (A. van Cleeff), w.pieters@utwente.nl (W. Pieters), r.j.wieringa@utwente.nl (R. Wieringa), frits.van.tiel@tunix.nl (F. van Tiel).

1363-4127/$ – see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.istr.2011.08.003

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

In practice these two trends blur: virtualized systems are given physical components, and CPS are being virtualized. An example of the first trend is cloud computing, which depends heavily on virtualizing resources that are shared among cloud users. The deficiencies of digital security[1] mechanisms, such as password reset via email, have led cloud vendors to start providing their users with hardware tokens (Amazon Web Services, 2010). Researchers are also investigating means to improve cloud security in the data center itself through specific hardware solutions (Berger et al., 2010). In effect, these cloud vendors and researchers are thus constructing cyber-physical systems. Examples of the second trend are industrial SCADA systems (Daneels and Salter, 1999) that control physical equipment at plants. These systems used to be spread among different physical servers that each execute a specific function such as database storage or PLC control. To increase manageability and save cost, at least one SCADA vendor has started to virtualize these systems onto one physical machine (van Cleeff, 2010), with unclear security consequences. Considering such cases, in which designers can choose between physical and digital implementations, there is a need for a more integrated risk assessment and design method that explicitly considers the benefits and limitations of physical and digital security mechanisms. The aim of this paper is to contribute to the creation of such methods, by extracting simple guidelines from our empirical case studies of virtualization in data centers. We examine the security consequences, what happens when physical mechanisms are replaced by digital mechanisms, and what combinations are possible. Specifically, we attempt to answer three questions:

1. What are the security properties of physical and digital security mechanisms?
2. Under what circumstances is virtualization technology secure?
3. How can physical and digital security be combined?

Our answers do not result in new techniques, but in knowledge of which we have seen that it is useful for performing trade-off analysis; system architects and IT security managers can use it to improve system security.

First Section 2 contains a short introduction to virtualization. Section 3 discusses related work concerning virtualization and physical security. Next Section 4 explains our data collection method, Section 5 contains the results, and we conclude in Section 6.

2. Virtualization

We will start with explaining the concept of virtualization, which we define as a software layer that implements a physical architecture (van Cleeff et al., 2009). The layer exposes an interface to other systems, effectively decoupling them from the hardware, which can improve portability, resource sharing and management. The systems running on top of the virtualization layer depend less on hardware specific implementations. We can divide virtualization by the state of the data that is affected: data in transit (network virtualization), data at rest (storage virtualization) and data in processing (server virtualization).

Network virtualization is possibly the most common type of virtualization: instead of placing individual cables between servers, cables are relayed to central switches, where digital separations are made between network sections. The second type of virtualization is storage virtualization. Data are no longer stored separately on individual hard disks but in a centrally managed storage array network (SAN), of which each server receives a part. Finally with server (or machine) virtualization, operating systems are presented with a virtual CPU. The software layer exposing this CPU is called the virtual machine monitor (VMM) or hypervisor. The VMM allows the physical server to be shared between multiple operating systems at the same time. Multiple servers equipped with VMMs can be bundled together to form virtualization clusters, and virtual machines can migrate between these servers, to optimize server load and maintenance schedules. Table 1 shows an overview of these types of virtualization.

In practice these types of virtualization are often used together. Machine virtualization also requires storage virtualization (the operating system must be loaded from disk) and a physical network connection must be virtualized to be shared between each operating system. The combination of all these virtualization technologies results in very complicated interaction patterns. For example in an implementation of one vendor, a virtual machine (VM) migration from one physical machine to another leaves the data (stored in the SAN) in the same place. However, the virtual network switches are still replicated over these physical servers.

3. Related work

In this section, we introduce related work about virtualization and CPS security, explain how we build on it and how our approach differs from existing approaches.

3.1. *Virtualization security*

There is an extensively list of literature on virtualization security (Vaughan-Nichols, 2008; Kim, 2008; Hoesing, 2009). Previously we performed a systematic review of security problems of server virtualization (van Cleeff et al., 2009). We concluded that virtualization technology can potentially improve availability, but that the likely effects on confidentiality and integrity are mixed. Most literature (including our own) examines technical issues, but to the best our

Table 1 – Overview of virtualization types.

Type	Physical component	Virtualized component
Storage	Hard disk	SAN
Network	Cross-cable	Switch
Machine	Rack server	VMM/Hypervisor

[1] The term 'logical security' is also widely used. For consistency, we will use the term 'digital' instead of 'logical' in this paper.

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

Table 2 – Data collected from case studies. D = documentation, I = interview only.

Activities and data obtained	X	Y	Z
Interviews with administrators	I	I	I
Interview with IT risk managers	–	–	I
Network architectures	D	D	I
List of physical servers	D	D	I
Data center layout	D	D	I
Security audit results	–	D	–
Installation procedures for servers	D	D	I

knowledge, virtualization security has never been researched by comparing physical and digital security mechanisms, which is the core topic of this paper.

Apart from scientific studies, VMM vendors such as VMware have also written extensively on virtualization security, guiding enterprises on how to perform infrastructure hardening (VMware, 2007) and server configuration (VMware, 2010). General advice is that virtual machines should be secured as physical machines, and be equipped with intrusion detection systems and anti-virus. However at a higher and more conceptual level, a VM cannot be secured in the same way, because - as is the thesis of our paper - there are differences between physical and digital security.

3.2. *Complementing digital security*

Another body of related work concerns the means to 'anchor' IT systems to the physical environment: when the existing infrastructure is too volatile, it needs to be 'grounded' into physical processes, forcing it to go through a specific physical location or device (Denning and MacDoran, 1996). In the context of location-based access control, we found that these studies are seldom explicit about how security precisely benefits from integrating with the physical environment (van Cleeff et al., in press). Other examples of cyber-physical mechanisms are the aforementioned hardware tokens, physical captchas (Golle and Ducheneaut, 2005) and hardware-based combinations of virtualization (Perez et al., 2008).

3.3. *Cyber-physical system security*

Security challenges are also discussed in the context of mainstream CPS research (Anand et al., 2006; Krogh et al., 2008). Problems include user privacy, as CPS typically gather data from sensors (which might be traced back to individual users), jamming of communications and trust. The NSF report of the 2008 CPS summit explicitly calls for an understanding of how to compose CPS, taking into account their physical and computational properties. (NSF, 2008) Cárdenas et al. investigate points of attack in a typical CPS, consisting of a physical system and a controller with feedback loop (Cardenas et al., 2008).

3.4. *Effects of automation on security*

Finally more theoretical research exists about effects of automation on security, and the differences between physical and digital systems. Blakley sees this mainly as a difference between inherent and imposed properties (Blakley, 1996). Physical systems have inherent properties, whereas digital systems have imposed properties. He gives the example of cash: in physical form it is hard to steal millions of dollars, whereas in digital form this can mean as little as swapping several bits (without this change being detected). In the context of privacy, Floridi coined the term 'ontological friction', meaning the forces that oppose information flow (Floridi, 2005). Automation reduces the difference between processors and the processed: digital programs can easily deal with digital data, which is not true of their physical equivalents. Alternatively, ICT offers the opportunity for privacy enhancing technologies as well. In this paper we will investigate the nature of these inherent and imposed properties, and assess if there is indeed less ontological friction in virtualized infrastructures.

4. Method

We will describe our research methods and design. First, we began with a literature study, which was published earlier in 2009 (van Cleeff et al., 2009), where we focused on the technicalities of virtualization security. Next we performed case study research, which we will describe in more detail.

4.1. *Sampling and data collection*

From 2009 to 2010 we performed case studies at three organizations. These are:

- X, an organization servicing over 5000 internal and external users;

Table 3 – Control categories in relation to CObIT definitions.

Category	CObIT	Explanation
Redundancy	DS4 Ensure Continuous Service	Ensure that there is no single point of failure.
Partitioning	DS5.10 Network Security	Separate systems to limit propagation of undesired events.
Access control	DS5.3 Identity Management, DS5.4 User Account Management	Ensure that only authorized personnel has access.
Work instructions	DS5.2 IT Security Plan	Provide detailed and precise instructions so that changes are executed correctly.
Monitoring	DS5.5 Security Testing, Surveillance and Monitoring	Log system events and check for undesired events.

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

Table 4 – Physical and digital procedural equivalents.

Procedure type	Physical procedure	Digital procedure
Network	place cables between switches and servers	configure switches, VMM, operating system, firewall
Storage	add/remove disks	configure SAN, VMM, operating system
Processing	add/remove CPUs, memory, motherboards	configure VMM, operating system
Application	install using monitor, keyboard and mouse	install from remote console or VMM

- Y, a financial service provider with over 100 million Euros in assets;
- Z, a payment service provider.

These organizations were selected based on expressed interest in participation and accessibility, and range from having a very limited interest in security (X) to being extremely concerned about security (Z). (See Section 4.3 for a discussion of the validity of the results.)

We developed a case study protocol with detailed questions, and we performed in-depth interviews with administrators and risk managers, and obtained documentation concerning the architecture and management of the organizations' data centers. Research was done under NDA, after which participants approved publication. Typically we met with our case study partner once, except for case *X*, where three interviews were done. Table 2 shows which types of data were obtained for each case. The amount of data that could be collected varied from case to case, depending on time constraints of IT staff, third parties involved, and concerns over the security consequences of the research itself.

4.2. *Data analysis*

In order to analyze the data, we have used part of CObIT (IT Governance Institute, 2007), which provides a framework for managing IT processes. In a top-down approach, an enterprise must state its business and IT goals, the processes that contribute to these goals, and the *control objectives* for these processes. Controls are the business processes (policies, procedures, practices) that provide assurance that business objectives are achieved and if not, that undesired events are prevented and/or detected. For the analysis, we used five broad categories of controls shown in Table 3.

As for the comparison between physical and digital processes, digital processes always have a physical basis - we cannot configure a VMM if there is no hardware to execute it upon. However, for digital procedures, hardware installation is a one-time event, after which everything can be done digitally, without modifying the hardware. Thus, in effect, we compare physical procedures with digital procedures *after hardware has been installed*.

We have thus investigated:

1. the types of processes or procedures that the participants execute
2. the physical and digital equivalents of these processes
3. the control objectives for these processes
4. the differences between physical and digital control objectives
5. the properties or mechanisms underlying these differences

4.3. *Validity*

Concerning the internal validity of our study, we took effort to guard this, sending our initial results to each participant and made several corrections or additions hereafter.

Regarding the external validity, our sampling method was theoretical, with the intention to select cases that were of theoretical interest. We especially took effort to include an organization that was extremely security-conscious, because we anticipated that important security problems of virtualization were only be noticeable in such a situation. With a theoretical sampling method, results are generalizable, not because of statistical sampling techniques, but because the *mechanisms* identified in these case studies are generalizable for the entire population of cases.[2] Translated to our study, this means for example that the controls and properties are present in any organization that uses virtualization technology. Regarding the systems studied, all our participants used variants of VMware's ESX, which is the market leader for virtualization software.

5. Results

This section presents the results of our case studies. First, we demonstrate that there is indeed a choice to be made between executing physical and digital procedures. This is shown in Table 4, where we group procedures found in one or more of our case studies under four broad types. The first three concern infrastructure management, and are network, storage and processing. The fourth category is application management, the installation and configuration of applications.

Having presented physical and digital procedural equivalents, we will now discuss the *controls* for these procedures, the mechanisms that provide reasonable assurance that business goals are met - in this context the goals of the confidentiality, integrity and availability of these systems. Table 5 shows the controls found in our case studies, demonstrating that for each control category physical and digital equivalents exist.

5.1. *Properties of physical and digital security mechanisms*

We will now investigate the differences between physical and digital security mechanisms. First, we present the evaluation of these controls based on interviews with our case study

[2] For more information about generalization from case studies, we refer to Pawson and Tilley (Pawson and Tilley, 1997).

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

Table 5 – Physical and digital controls.

Control category	Physical control	Digital control
Redundancy	redundant physical structures	snapshots, dynamically migrate machines
Partitioning	separate systems physically data centers in different locations out-of-band management connections	system separation using firewalls, switches limit snapshots and replication separation of duty in access control
Access control	card for physical access underground cables locks on server cabinets	digital access control
Work instructions	standard operating procedures different colors and labels for cables, port numbers, switches	scripted changes naming conventions
Monitoring	surveillance of persons visual server inspections surveillance cameras in data centers visitors accompanied in data centers	logging, monitoring, auditing dual control

participants. With these results, we contrast physical to digital security controls, to find their main differences and properties. We then use these properties to explain the different effects of physical and digital security.

In general, case study participants have a mixed view on physical security mechanisms. Physical security is seen as 'harder' than digital security and also more static, being more difficult to change. Good physical separation requires different physical locations or rooms. However, even though separation through cables is possible, assessing if this is done properly is difficult because cables can be very long. Separating systems or storing passwords is done best with physical security. Physical procedures are visible and are executed and verified by persons on location in the data center. Participants also point out that sending someone into a data center has inherent risks, as she can physically do more then she is entitled to, and this cannot always be observed easily.

In contrast digital security is considered to be 'neater': it gives more control and precision for granting authorizations, and digital changes are executed directly and uniformly and can be scripted remotely. Furthermore, it allows better logging and auditing. In fact continuous monitoring is a necessity: if monitoring is not in place, virtualization causes extra risks, because the infrastructure is much more volatile, a configuration found at one time can easily have been different before, or be altered after. A drawback of digital security is also that it is not visible.

Table 6 summarizes these evaluations of physical and digital controls and we use these to sum up key differences between properties of physical and digital systems in Table 7. Physical controls depend on the inertness of physical systems - if untouched they remain intact. Also, physical systems are visually inspectable. By contrast, digital systems are volatile by nature; systems can reconfigure themselves to improve security, but the state itself cannot be observed directly. Physical and digital systems also differ concerning the execution of changes: physical changes require force and are less precise than digital changes, and change history is harder to track.

Next, we use these differences to explain how these properties relate to the controls categories. Table 8 presents this explanation.

Our conclusion is that redundancy and partitioning are both good control strategies in the physical and digital world, but that access control can be more precisely regulated in the digital world than in the physical world. Work instructions are not a reliable control strategy in the physical world. Monitoring is more effective in the digital world and actions can be logged easier. We have observed these properties of physical and digital controls in our cases but because they are explainable by general properties of the physical and digital world (Table 8), they are generalizable to other cases too.

5.2. *Secure application of virtualization technology*

We can now investigate to what extent physical controls can be replaced by digital controls - is there a limit to what can be virtualized securely? We will answer this question starting with the business goals that participants wished to achieve. First, the main two reasons given by our case study

Table 6 – Properties of physical and digital controls.

Control category	Physical control property	Digital control property
Redundancy	static	dynamic reallocation
Partitioning	hard	soft
Access control	unrestricted access	more precision
Work instructions	changes both digital and physical, cables hard to trace	more precision, direct and uniform changes, remote scripting
Monitoring	cables hard to trace cables visible unrestricted access	(forget) auditing

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

Table 7 – Main differences between physical and digital properties.

Aspect	Physical	Digital
visibility	yes	no
volatility	low	high
precision of change	low	high
change effort	high	low
change history	none	Yes

participants for using virtualization were improving availability of their systems and reducing hardware cost. These two benefits were realized by virtualization, and as such virtualization has no limit.

However, virtualization did not always contribute to confidentiality. First, security problems had existed with the virtualization infrastructure at organization Y: because of switch and firewall misconfigurations, the management network for the infrastructure was available outside the management domain, thus removing the digital partitioning. Secondly, auditing of the virtualization software was not implemented. Organization Y and Z were concerned about data leakage, and locked down the VMM management tools to achieve this, limiting snapshot making of virtual machines to a specific group of administrators, or in case of organization Z, prohibiting replication and snapshot making completely.

Of specific concern for organization Z were hardware security modules (HSM). These devices are used for storage of cryptographic keys and the encryption and decryption of data using these keys. To prevent tampering, they are physically secured by motion detectors and light sensors. In effect, an HSM is thus also a CPS. Can such a device be virtualized as well, and if not, can it securely connect to a virtualized infrastructure? We conclude that virtualizing an HSM is possible but will result in a bigger space that must be secured physically - not just the HSM but the entire data center. Obviously, an HSM is easier to manage and this indicates a limit to the benefits of virtualization.

A more fundamental argument to the question of virtualization's limits can be given by observing that both availability and confidentiality have their roots in the physical environment: confidentiality as in the case of HSMs data depends on keys (which must be physically and digitally confined). By contrast, availability of data requires multiple data centers in different locations and connections between them, to ensure continuous operation. As such there is an inherent conflict between these two, and virtualization (connecting and integrating systems) naturally favors availability over confidentiality.

We conclude that there are indeed practical limitations to virtualization: the more is virtualized, the tighter an organization must manage the virtualized and physical infrastructure to meet confidentiality requirements.

Table 8 – Effect of physical and digital properties on control objectives.

Control category	Physical	Digital
Redundancy	+ inert	+/− volatile
Partitioning	+ inert	+/− volatile + precise
Access control	− imprecise + force required + inert	+ precise + controlled
Work instructions	− imprecise − force required	+ controlled
Monitoring	+ visible − no history	− invisible + history

5.3. *Existing combinations of physical and digital security*

To answer our third research question about combining physical and digital security, we will specifically examine mechanisms for separation of virtualized servers. As mentioned, all digital security ultimately depends on physical security. Case study participants setup their data center in two steps: first install and connect all servers physically in one zone, and second separate systems inside these zones using firewalls and enable necessary connections between the servers. A change in the firewall policy does then not require data center access, but can be done remotely. The order of changes is important: digital changes do normally not require physical changes, whereas a physical change would require digital reconfiguration.

Our investigation shows that there are four basic types of separation:

1. Physical separation.
2. Physical separation enabled by digital configuration.
3. Digital separation.
4. Digital separation enabled by physical configuration.

First, physical separation is the first line of defense: servers are physically separated in zones that are disconnected and sometimes also have different physical access controls, for example a server cabinet with a lock. Virtual machines can only migrate inside these zones. Servers have out-of-band channels for remote console access through a separate network connection. Second, servers and switches are configured to make sure that management access is only possible through specific physical channels. In the case of VMM servers, the management interface is digitally connected to a specific physical network card, which is then linked to the maintenance domain, routing the traffic over a specific physical network cable. Third, separations between servers are done through digital configurations. In the products used by our participants, administrators can define and connect virtual switches to different virtual machines. Fourth, digital access can also be physically secured: ideally, out of band access is only possible from physically secured locations.

Fig. 1 shows a simplified configuration of virtualized servers as we encountered in our case studies. We have two physical servers 01 and 02 equipped with several physical network connections (NIC 01 through 05). The servers are connected through two physical switches 4 and 5. On the physical server 01, three virtual machines are running. Virtual machines are also connected to the network via virtual switches (Switch 1 through 3).

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

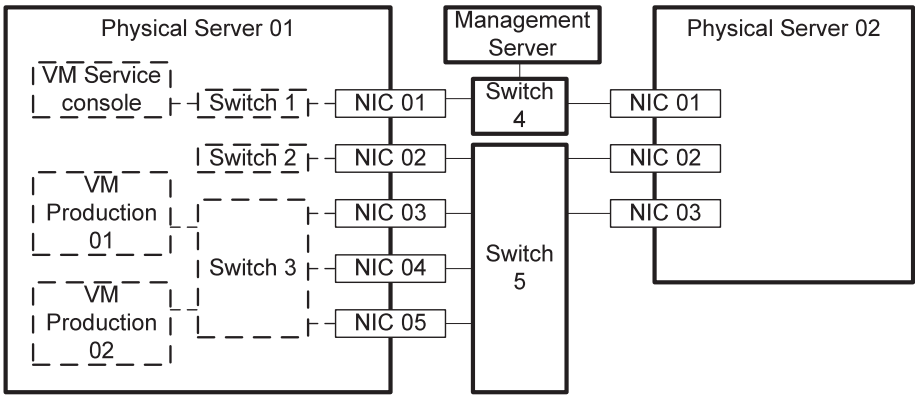

Fig. 1 – Physical and virtual connections.

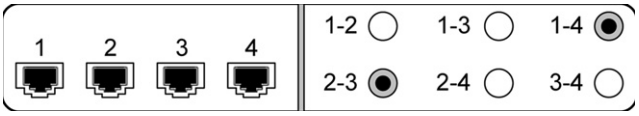

Fig. 2 – Schema of a physically configurable switch.

Because of the differences in security properties found in Section 5.1, combining physical and digital security has the potential to improve security. However, it has also the potential of being less secure than either physical or digital security mechanisms. In the example of Fig. 1 we observe that the system is digitally configured such that the management console is only accessible from the management server via switch 4. Thus the management network traffic is physically separated, as the normal VM traffic occurs via switch 5. However if the virtual switches 1 and 2 are merged by a digital change such as an attack or in a misconfiguration accident, the management traffic can also occur via switch 5 and physical separation loses its value. Thus type 2 physical separation is less hard than type 1 separation.

5.4. *New combination of physical and digital security mechanisms*

We will now give one example of how our results can be used to construct new security mechanisms, based on the problems identified in our case studies. With existing technology, network connections can be either configured digitally (through a switch) or physically (through a patch cabinet). The former has the disadvantage of being changeable easily, whereas the latter is hard to audit because cables need to be followed. However physical and digital properties can be combined in new ways, by making a switch that is physically configurable, providing much more rigidity than current digital solutions, while still allowing for auditing and monitoring.

An example of such a switch is shown in Fig. 2, where servers 1 and 4, and servers 2 and 3 are connected, indicated by the dark color of the (enabled) buttons on the right. Such a switch uses a new mixture of physical and digital separation, and combines the most beneficial properties of the physical and digital domain as shown in Table 9.[3]

Table 9 – Beneficial physical and digital properties of the proposed switch.

Domain	Property	Explanation
Physical	force required	Changes require a physical presence.
	inert	After clicking, the buttons remain in the same position.
	visible	The active network connections can be visually inspected.
Digital	precise	The buttons are clearly indicated, it is not necessary to swap cables in a patch cabinet.
	history	The switch can record the button clicks.

6. Conclusion

Our case study research on virtualization revealed benefits and limitations of physical and digital security mechanisms. Physical mechanisms are especially beneficial when few changes are made to systems, whereas digital mechanisms are preferred when systems are very dynamic. However, digital misconfigurations are always possible, and for every physical security mechanism to be replaced by a digital mechanism, the monitoring and auditing requirements increase substantially.

The realization of system availability is at odds with confidentiality, and as virtualization connects systems, it favors availability. These findings have consequences for our view on cloud computing, which depends heavily on virtualization technology; Ensuring confidentiality in a cloud environment requires more effort compared to a non-virtualized environment.

Furthermore, existing technology limits effective combinations of physical and digital security mechanisms. Currently, these combinations lead to an overly heavy reliance on digital security mechanisms, negating positive effects

[3] In its current form, the switch lacks an authentication mechanism. We imagine that a more advanced version could use a smartcard feature for this.

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003

of physical security. Smarter combinations can be made, and we have shown how our findings can be applied to construct new and better security mechanisms, giving an example of a new type of switch.

Concerning physical and digital security tradeoffs, because our research was limited to virtualization in private clouds we see the investigation of other CPS and public clouds as future work.

Acknowledgments

We wish to thank our anonymous case study partners for allowing us access to their organizations, spending time to answer our questions and commenting on earlier drafts of this paper. This research is supported by the research program Sentinels (www.sentinels.nl). Sentinels is being financed by Technology Foundation STW, the Netherlands Organization for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs under project number TIT.7628.

REFERENCES

Amazon Web Services. Amazon Web services: overview of security processes, http://awsmedia.s3.amazonaws.com/pdf/AWS_Security_Whitepaper.pdf; 2010. retrieved 11.06.10.

Anand M, Cronin E, Sherr M, Blaze M, Ives Z, Lee I. Security challenges in next generation cyber physical systems. Beyond SCADA: Networked Embedded Control for Cyber Physical Systems; 2006.

Berger S, Cáceres R, Goldman K, Pendarakis D, Perez R, Rao J, et al. Security for the cloud infrastructure: trusted virtual data center implementation. IBM Journal of Research and Development 2010;53(4):6.

Blakley B. The emperor's old armor. In: Proceedings of the 1996 workshop on new security paradigms. ACM; 1996. p. 2–16.

Cardenas A, Amin S, Sastry S. Secure control: towards survivable cyber-physical systems. In: Distributed computing systems workshops, 2008. ICDCS'08. 28th international conference on. IEEE; 2008. p. 495–500.

van Cleeff, A.: Personal communication (2010)

van Cleeff A, Pieters W, Wieringa R. Security implications of virtualization: a literature study. In: 2009 International conference on computational science and engineering. IEEE; 2009. p. 353–8.

van Cleeff, A., Pieters, W., Wieringa, R.: Benefits of location-based access control: a literature study. In: Proceedings of the 2010 IEEE/ACM Int'l Conference on Green Computing and Communications & Int'l Conference on Cyber, Physical and Social Computing. Washington, DC, USA: IEEE Computer Society; 2010. p. 739–746.

Daneels A, Salter W. What is SCADA?. Trieste, Italy. In: Proceedings on the international conference on accelerator and large experimental physics control system; 1999.

Denning D, MacDoran P. Location-based authentication: Grounding cyberspace for better security. Computer Fraud & Security 1996;1996(2):12–6.

DePoy J, Phelan J, Sholander P, Smith B, Varnado G, Wyss G, et al. Critical infrastructure systems of systems assessment methodology. SAND2006–6399. Sandia National Laboratories; 2006.

Floridi L. The ontological interpretation of informational privacy. Ethics and Information Technology 2005;7(4):185–200.

Golle P, Ducheneaut N. Preventing bots from playing online games. Computers in Entertainment (CIE) 2005;3(3):3.

Hoesing M. Virtualization security assessment. Information Security Journal: A Global Perspective 2009;18(3):124–30.

IT Governance Institute. CObIT 4.1. Rolling Meadows, IL 60008 USA: Isaca; 2007.

Kim G. Seven steps to a secure virtual environment. Network Security 2008;2008(8):14–8.

Krogh B, Lee E, Lee I, Mok A, Rajkumar R, Sha L, et al. Cyber-physical systems, executive summary; 2008.

NSF. Report: cyber-physical systems summit, http://varma.ece.cmu.edu/Summit/CPS_Summit_Report.pdf; 2008. retrieved 21.03.10.

Pawson R, Tilley N. Realistic evaluation. Sage Publications Ltd; 1997.

Perez R, van Doorn L, Sailer R. Virtualization and hardware-based security. IEEE Security & Privacy 2008;6(5):24–31.

Vaughan-Nichols S. Virtualization sparks security concerns. Computer 2008;41(8):13–5.

VMware. VMware infrastructure 3-security hardening, http://www.vmware.com/pdf/vi3_security_hardening_wp.pdf; 2007. retrieved 31.10.10.

VMware. ESX server 3 configuration guide, http://www.vmware.com/pdf/vi3_35/esx_3/r35/vi3_35_25_3_server_config.pdf; 2010. retrieved 11.01.10.

Please cite this article in press as: van Cleeff A, et al., Integrated assessment and mitigation of physical and digital security threats: Case studies on virtualization, Information Security Technical Report (2011), doi:10.1016/j.istr.2011.08.003