INTEGRATING INFORMATION ASSURANCE INTO SYSTEM ADMINISTRATION

Erik Hjelmås[1], Nils Kalstad Svendsen[1], Stephen D. Wolthusen[1,2]

[1]Norwegian Information Security Laboratory
Department of Computer Science
Gjøvik University College
N-2818 Gjøvik
Norway

[2]Information Security Group
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey TW20 0EX
United Kingdom

[1]{erikh,nilss}@hig.no, [2]stephen.wolthusen@rhul.ac.uk

ABSTRACT

While the cost and flexibility benefits resulting from distributed and cloud computing environments are clearly evident, this approach also has far-reaching implications for the threat surface presented as well as general information security risks, particularly to availability. The design of cloud-based storage services also implies that data once stored with such services may very hard to recall. The ease with which these services can be used implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture unless the implications are understood clearly. As the impact is both technical and legal in nature and can easily have a temporal extent well exceeding the life-time of a given configuration, we argue that the professional education of system and network administrators must take these security aspects into consideration even at the undergraduate level. We therefore outline a curriculum integrating information security and security management topics into a 3-year (180 credit points in the European Credit Transfer System) Bachelor of Science degree in Computer Science

with specializations in either *Network and System Administration Operations* or *Information Security* intended to enable students to create, operate, and maintain information systems not only fulfilling functional, efficiency, and robustness requirements, but also minimizing information security and liability risks.

KEY WORDS

Security Architecture, Curriculum Design, Information System Architecture

INTEGRATING INFORMATION ASSURANCE INTO SYSTEM ADMINISTRATION

1 INTRODUCTION

The ability to construct virtual information systems either locally or using a wide range of options from externalizing individual services to a fully distributed or cloud computing [2] environment rapidly implies that system administrators may not only be called upon much more frequently to make decisions that would previously have been the prerogative of system architects, but that such decisions may be based more on momentary expediency than sound architecture as it may be faster and more cost-effective to call upon an external service provider than to bring internal services on-stream [4]. Moreover, the use of services rather than capital equipment and the prospect of off-loading most of the administrative responsibility associated with such services all provide strong incentives at levels from system administrators to system architects.

The use of such facilities does, however, involve a number of risks both technical and legal in nature which must be fully understood as some of the consequences of service use are difficult if not impossible to reverse and hence can have a temporal extent that far exceeds the life-time of a given configuration. At the same time it is unlikely that, as requirements emerge at the operational level, decisions on how to meet requirements will be escalated to a strategic system architect's level at all time. Given that many such services are, however, interdependent on each other either directly or indirectly, even a small number of externally provisioned services can represent a long-term commitment.

Because of this, we argue that system and network administrators even at the operational level, where first-line responsibility is likely to reside with staff holding undergraduate or professional degrees, must increasingly have a solid understanding of network and service architecture and the information security and security management implications, making distinctions in degrees and pathways increasingly questionable. Based on these observation and the fact that the European Higher Education Area (also known informally as the *Bologna system*) offers a flexible mechanism for structuring degree programs in a modular fashion, we propose to adapt curricula in the computer science area in such a way that students wishing to specialize in

system architecture and management or professionals intending to update their qualifications can do so in a cohesive and integrated manner.

The remainder of this paper is therefore structured as follows: Section 2 briefly reviews the types of services and facilities available to information system architects and administrators, while section 3 discusses the information security implications resulting from these developments. Based on this, sections 4 and 5 then derive a set of requirements for integrating information security into undergraduate programs for information system administration and architecture and a proposed approach for meeting such requirements within the scope of ACM/IEEE curriculum recommendations, followed by a discussion on ways of enhancing the mobility of graduates both geographically and particularly along career pathways in section 6 and brief conclusions in section 7.

2 DISTRIBUTED AND CLOUD ENVIRONMENTS

Distributed computing services are, despite recent and periodic re-naming and different efforts at promoting such services, has been a long-standing vision arguably originating with the *Computing Utility* proposed by the MIT MAC project [5] as articulated by Fano and subsequently implemented substantially in the Multics system [3]. It is particularly noteworthy in this context that one of the core concepts of modern cloud computing, i.e. the sharing and remote commercial use of virtual machines dates to the mid-1960s. In the following, section 2.1 briefly reviews some of the key features of current distributed computing architectures, while section 2.2 highlights systems management aspects of such architectures.

2.1 Distributed Computing Platform Components

While terminology varies considerably, a simple taxonomy of distributed computing elements can be derived based on the granularity of the services offered. At the finest level of granularity, individual services, typically web or database services (currently being referred to as *applications in the cloud* or AITC) are providing business processes or components with state distributed across servers and client systems. Several implementation variants, frequently hybrid, ranging from legacy CORBA environments via SOAP and WS infrastructures [14] to AJAX [8] based on the design principle of representational state transfer (REST) originally articulated by Fielding [6].

Each service may in turn depend on others and can require several service layers (frequently employing database back-ends). Moreover, a number of ancillary services can be required, including service discovery mechanisms, name services and, when security mechanisms are utilized, key management infrastructures. Moreover, each of these services can be provided in a geographically distributed manner, adding the interconnecting networks to the infrastructure required for provisioning such services. While general deployment of such services is limited, some areas such as externally provisioned email services are increasingly common.

Similar design principles employing middleware components are also found in more complex service-oriented architectures in which complex business processes are composed of multiple implementation services and events typically coordinated on enterprise service bus responsible for process choreography and service orchestration [13]; this is also referred to as *platforms in the cloud* (PITC). Software as a service (SaaS) as originally described by Bennett *et al.* [1] can be considered a derivative of this approach in that the service delivery uses the same technical underpinnings while state is typically retained on the application service provider's systems; infrastructure dependencies are therefore potentially of similar complexity as in the case of uncoupled web services. However, the most popular approach commonly associated with the term cloud computing (also referred to as *infrastructure in the cloud*, IITC) is of a more coarse granularity in that it is centered on the provisioning of virtual machines and storage space available commercially from a number of sources [10]. Although this eliminates some of the interdependency layers noted above, access to services will still require queuing, network and cryptographic key management as well as potentially front-end infrastructures, while both virtual machines and storage will frequently be re-located dynamically to provide improved response times and failure tolerance as well as load balancing.

2.2 Cloud Management

Although particularly in case of IITC residual system management responsibility lies with the service user and network as well as enabling infrastructure must still be maintained, significant portions are migrating to the infrastructure provider. This requires not only the elaboration of service level agreements (SLA) for all relevant aspects of the service, but also monitoring compliance with SLAs and the deployment of mitigation and service level

enforcement mechanisms [12].

3 SECURITY CHALLENGES

A number of security issues arising from the distributed environments outlined in section 2 are easily identified. While securing confidentiality and integrity of data in transit is trivially addressed using standard cryptographic protocols, even storage presents a number of difficulties as encrypting data at rest may both interfere with desired functionality and adversely affects application performance. Moreover, as data is processed, by definition, on systems under the control of one or more third parties, it will be available as plaintext in such an environment. This raises questions both about the trustworthiness of service providers and the strength of compartmentalization between virtual machine instances, which must not only be maintained during operation but also in case of virtual machine migration [16].

Further security issues arise from uncertainties about the integrity of the computing and communication platform themselves, which can affect the integrity of both the applications and that of active monitoring, e.g. by Byzantine behavior in suppressing or altering messages. This type of threat is also present for the case of key and identity management; as key material is implicitly exposed, it may be accessible to adversaries at endpoints or within the management infrastructure of the service provider.

Given the exposure of network traffic as well as potential cross-service contamination and hence the increased risk of denial of service attacks compared to systems within an organization's perimeter, availability is a major security consideration. While reliability models can provide predictable high levels of availability in the face of random (Gaussian) failures, this may not be the case for deliberate attacks, which may indeed target the very mechanisms providing robustness and redundancy such as load balancing mechanisms.

However, while the above touches upon several critical and in part insufficiently resolved security challenges in cloud computing, there are further implications for legal and management perspectives which must also be taken into account. In most backup configurations, multiple copies and generations of backup data are interspersed on storage media at different access hierarchies. While this redundancy is typically desirable in the event of failure, deletion of data sets such as in case of the termination of a service agreement is problematic, particularly if a service provider does not isolate backups for

different customers as is commonly the case and implied in terms and conditions of service providers. Similarly, both servers and storage media may be in different physical locations with services and data migrating among locations to provide optimum resource usage and service levels. However, while such migration and distribution is deliberately transparent at the implementation level, physical location can imply that a given datum or service may fall under different jurisdiction. In some cases this may even affect the legality of a service or transactions, but a major concern arises from the possibility of seizing evidence in criminal or civil proceedings as well as for compliance purposes. Moreover, certain processes may rule out the use of cloud computing environments entirely [11].

4 CURRICULUM REQUIREMENTS

Enabling students to make informed decisions on service provisioning and deployment and taking security considerations into account in network and system administration must be balanced with requirements for the core of the respective curriculum. In doing so, the structure of undergraduate degrees in the European Higher Education Area limits the ability to add modules as it defines a B.Sc. degree to encompass 180 credit points in the European Credit Transfer System (ECTS) over three years of studies. However, as will be shown in section 5, key aspects of the required knowledge can be incorporated in core modules of the computer science undergraduate degree, and can also provide a running theme which can be carried forward to the capstone project in the B.Sc. dissertation. This permits the concentration of specific aspects conjoining information assurance and system administration in selected elective modules, thereby providing students with the flexibility to choose their specialization area relatively late in the course of their studies or to combine the specialization areas of Network and System Administration (NSA) and Information Security (IS).

At the same time, the specialization areas are designed to be aligned with recognized standards and best practices in the respective areas; in the case of NSA, this is the Computing Curricula Information Technology (CCIT) [9], albeit with a stronger emphasis on technical capabilities. For IS, the alignment is with the Certified Information Systems Security Professional (CISSP) domains; once again, the focus here is more on technical aspects.

As several of the issues noted in section 3 also have legal aspects connected to them, this is incorporated in the form of elective modules. Either special-

ization area, however, provides a balance between the core computer science curriculum including a solid mathematical foundation [15] whilst establishing a solid foundation for subsequent postgraduate degrees, particularly specializing in information security either in direct succession to the undergraduate program or after a hiatus [7].

5 CURRICULUM DESIGN

While, as noted in section 4, all specialization areas are built around a strong computer science core and incorporate information assurance elements, the pathways and elective modules themselves differ, with the IS pathway providing further options to specialize in topics relevant to information assurance and security.

5.1 B.Sc. Information Security (IS)

The B.Sc. in computer science with its specialization in information security combines the core of a traditional computer science program with information technology and information assurance along with up to date knowledge and skills related to current information technology.

The core pathway is illustrated in figure 1; this is augmented by elective modules covering the CISSP core bodies of knowledge — Access Control (AC); Application Security (AS); Business Continuity and Disaster Recovery Planning (BCDR); Cryptography (C); Information Security and Risk Management (ISRM); Legal, Regulations, Compliance and Investigations (LRCI); Operations Security (OS); Security Architecture and Design (SAD); and Telecommunication and Network Security (TNS) — with the exception of Physical Security (PS), which are structured in the modules as shown below (several additional electives are not shown); here, the first digit denotes the year of the program in which these electives are typically chosen.

IMT3491 Ethical Hacking and Penetration Testing
IMT3551 Digital Forensics
IMT3771 Introduction to Cryptology
IMT3292 System Administration
IMT3281 Software Development
IMT3511 Discrete Mathematics
IMT2291 Web Technology

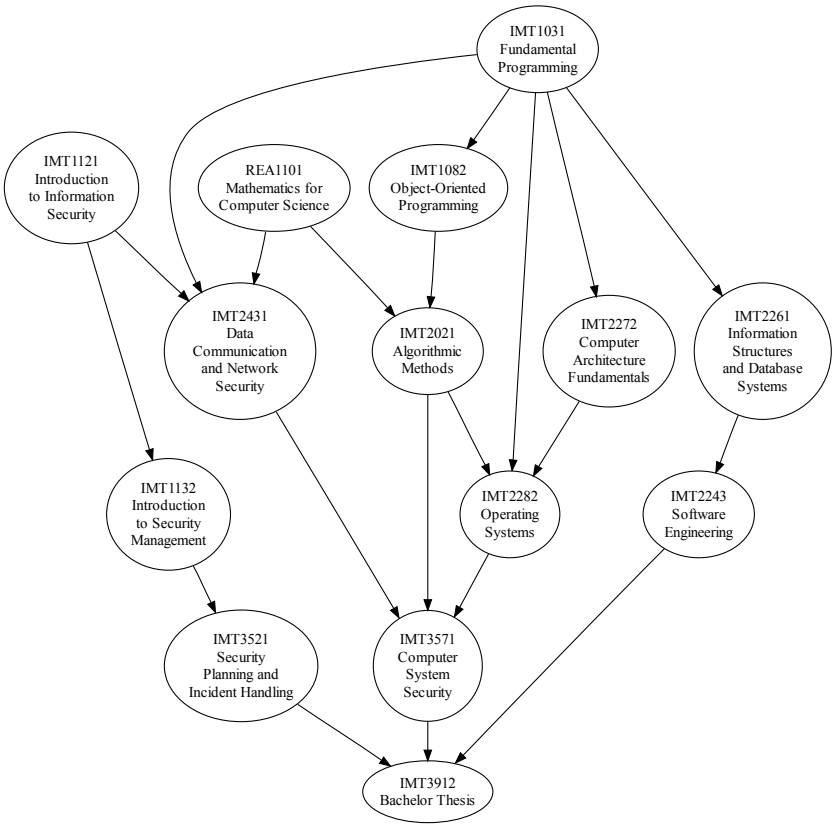

Figure 1: Module Interrelations in the IS Core Curriculum

IMT3441 Application and Database Management
SMF1042 Basic Economics
SMF2051 Organizational Management including Labour Laws
IMT1271 IT Service Management
IMT1321 IT Management

Figure 2 visualizes the coverage of these core aspects, where grey fields indicate partial, and black fields full coverage of the relevant subject areas.

5.2 B.Sc. Network and System Administration (NSA)

The B.Sc. with specialization in network and system administration (NSA) provides a more operationally-focused program compared to the IS specialization and is intended to provide the private and public sector with IT

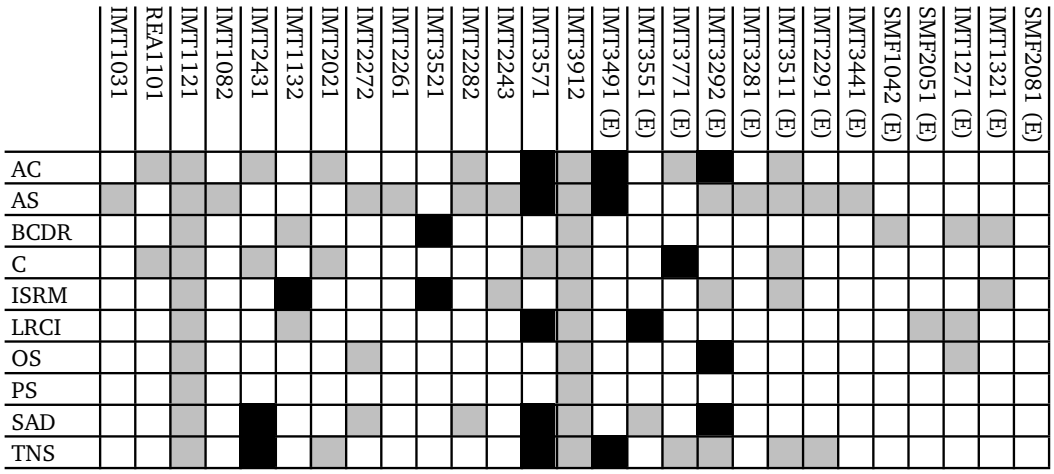

Figure 2: Matching CISSP Domains to IS Specialization Courses

professionals having a broad range of competence in evaluating and maintaining computerized infrastructures, and the ability to integrate a range of different technologies and their integration into an organization's structure.

Analogous to figure 1, the NSA core pathway is illustrated in figure 3, while the following list provides modules which are not already included in the elective roster shown in section 5.1:

IMT2072 Ergonomics in Digital Media
IMT1042 Basic Economics
IMT3102 Object-Oriented Software Development
IMT3571 Computer System Security
IMT1132 Introduction to Security Management
IMT3521 Security Planning and Incident Management
IMT3781 Introduction to Computer Law

While there is no immediate equivalent to the CISSP body for network system administration, the curriculum is aiming to cover the pervasive themes noted above and particularly makes reference to background knowledge required for a solid understanding of the ITIL (Information Technology Infrastructure Library) including the methods and skills required to successfully implement the best practices codified therein. In doing so, the NSA specialization aims to follow the *pillars-first* approach rather than the *integration-first* strategy advocated by CCIT, but aims to provide the strong

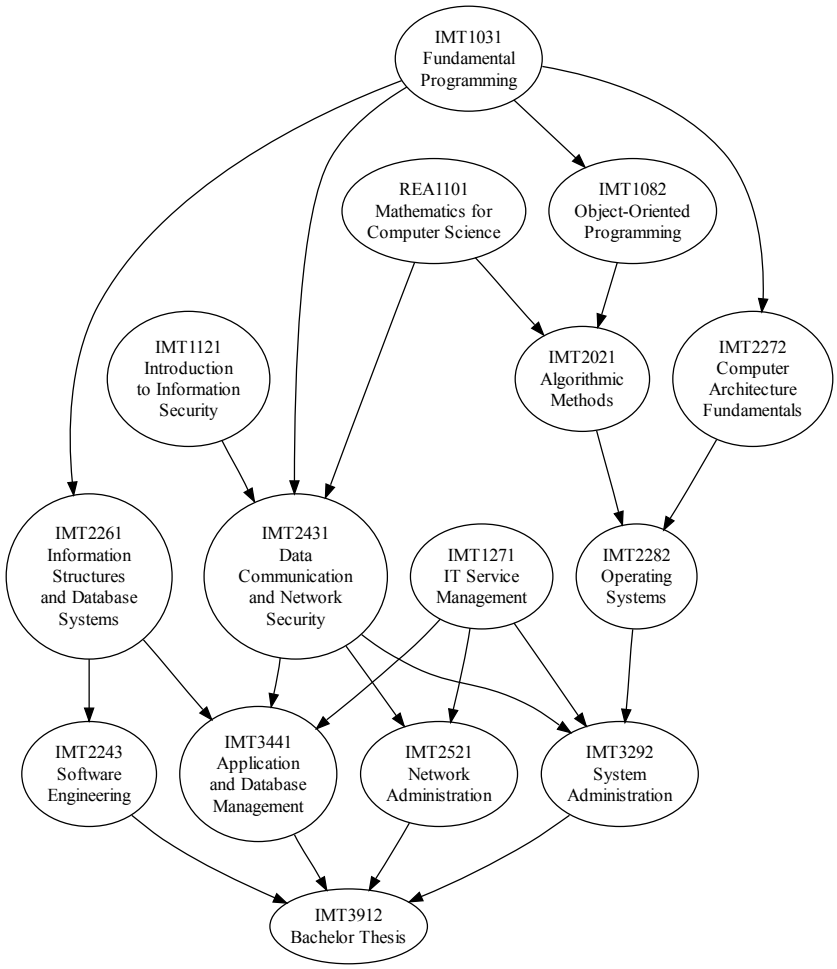

Figure 3: Module Interrelations in the NSA Core Curriculum

motivation that such an integration approach by using the topics described in sections 2 and 3 as the common theme without sacrificing technical depth in the process. At the same time, the program discussed here is, regardless of the specialization chosen, a more technically oriented program and eschews human-computer interaction and organizational issues, although these can be chosen as elective modules.

6 ENHANCING MOBILITY

Two areas of mobility are considered here, *career* and *international* mobility. An undergraduate degree as described in the present paper must fulfill dual purposes in that it simultaneously should prepare graduates for employment yet at the same time provide sufficient foundations and particularly introduce the methods of academic inquiry to enable suitably qualified candidates to proceed with postgraduate studies. We have outlined previously how students interested in information security and assurance are provided with opportunities at both the M.Sc. and Ph.D. levels in dedicated programs [7] and are deliberately structuring these postgraduate programs in such a way that they can also be taken in a part-time or low-residency format, making use of electronic media to provide interaction between students and faculty and among students where possible and scheduling lectures and seminars in a predictable manner, resulting in a desirable combination of continuing and mature students which can also contribute a professional perspective to fellow students. While the undergraduate program described here was, unlike the postgraduate programs, originally aimed primarily at domestic students, we are moving to provision all programs in English to allow better integration of international students. However, given the stronger emphasis on lectures, low-residency options are not considered feasible, although once again electronic communication forms are used extensively to support students. Given the diverse backgrounds of students, moreover, emphasis is placed on highlighting both common principles and possible divergences in areas such as legal courses.

7 CONCLUSION

In this paper we have described our approach to provisioning an undergraduate degree program in computer science which allows students to specialize in the critical areas of information security and network and system administration while at the same time neither sacrificing the technical foundations later enabling them to successfully pursue postgraduate programs nor the ability to become productive professionals. The common theme of distributed and cloud system assurance provides a strong motivational anchor which can encourage students to pursue topics without sacrificing depth as is commonly the case in integration-first courses. We have also carefully designed curricula to enable international and career mobility, showing clear pathways for

both academic and professional development in the information security and assurance area.

References

[1] K. Bennett, P. Layzell, D. Budgen, P. Brereton, L. Macaulay, and M. Munro. Service-based software: the future for flexible software. In *Proceedings of the Seventh Asia-Pacific Software Engineering Conference (APSEC 2000)*, pages 214–221, Singapore, December 2000. IEEE Press.

[2] R. Buyyaa, C. Shin Yeoa, S. Venugopala, J. Broberga, and I. Brandic. Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation Computer Systems*, 25(6):599–616, June 2009.

[3] F. J. Corbató and V. A. Vyssotsky. Introduction and Overview of the Multics System. In *Proceedings of the AFIPS Fall Joint Computer Conference (1965 FJCC)*, volume 27 part 1, pages 185–196, Las Vegas, NV, USA, November 1965. AFIPS, Spartan Books.

[4] M. Fan, S. Kumar, and A. B. Whinston. Short-term and long-term competition between providers of shrink-wrap software and software as a service. *European Journal of Operational Research*, 196(2):661–671, July 2009.

[5] R. M. Fano. The MAC System: The Computer Utility Approach. *IEEE Spectrum*, 2(1):55–64, January 1965.

[6] R. T. Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. PhD thesis, Department of Information and Computer Science, University of California, Irvine, Irvine, CA, USA, 2000.

[7] E. Hjelmås and S. D. Wolthusen. Full-Spectrum Information Security Education: Integrating B.Sc., M.Sc., and Ph.D. Programs. In *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, pages 9–16, Kennesaw, GA, USA, September 2006. ACM Press.

[8] A. T. Holdener III. *Ajax: The Definitive Guide*. O'Reilly, Sebastopol, CA, USA, 2008.

[9] B. M. Lunt, J. J. Ekstrom, S. Gorka, G. Hislop, R. Kamali, E. Lawson, R. LeBlanc, J. Miller, and H. Reichgelt. Information Technology 2008 — Curriculum Guidelines for Undergraduate Degree Programs in Information Technology (ACM/IEEE Computer Society. Technical report, Association for Computing Machinery, November 2008.

[10] J. Murty. *Programming Amazon Web Services*. O'Reilly, Sebastopol, CA, USA, 2008.

[11] Payment Card Industry. Payment Card Industry Data Security Standard: Requirements and Security Assessment Procedures. Technical report, PCI Security Standards Council LLC, October 2008.

[12] V. Stantchev and C. Schröpfer. Techniques for service level enforcement in web-services based systems. In *Proceedings of the 10th International Conference on Information Integration and Web-based Applications & Services (IIWAS 2008)*, pages 7–14, Linz, Austria, November 2008. ACM Press.

[13] S. Tarkoma. *Mobile Middleware Architecture, Patterns, and Practice*. John Wiley & Sons, Inc., Chichester, UK, 2009.

[14] S. Weerawarana, F. Curbera, F. Leymann, T. Storey, and D. F. Ferguson. *Web Services Platform Architecture*. Prentice-Hall, Englewood Cliffs, NJ, USA, 2005.

[15] S. D. Wolthusen. The Role of Mathematics in Information Security Education. In *Proceedings of the 5th IFIP TC11.8 World Conference on Information Security Education (WISE 5)*, pages 129–136, West Point, NY, USA, June 2007. Springer-Verlag.

[16] F. Zhang, Y. Huang, H. Wang, H. Chen, and B. Zang. PALM: Security Preserving VM Live Migration for Systems with VMM-enforced Protection. In *Proceedings, Third Asia-Pacific Trusted Infrastructure Technologies Conference (APTC '08)*, pages 9–18, Hubei, China, October 2008. IEEE Press.