© 2011 IEEE. Personal use of this material is permitted. Permission from IEEE must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works.

Digital Object Identifier: 10.1109/IWCMC.2011.5982533

A Virtual Network Topology Security Assessment Process

R. Goyette and A. Karmouch
School of Information Technology and Engineering
Faculty of Engineering – University of Ottawa, Canada
{goyette,karmouch}@site.uottawa.ca

***Abstract*— Network virtualization is a concept in which a Virtual Network Provider constructs logical virtual networks for various clients on a common, virtualized infrastructure substrate. However, there is currently no general framework or benchmark for assessing the security properties of these logical networks within the context of network virtualization. In this paper, we describe a virtual network security assessment process in which a preference model is constructed over a select set of network element attributes. This preference model reflects the knowledge and experience of one or more security experts. The relevant attribute values are exposed during virtual network composition. Our process answers the question: "how does the security of my virtual network compare to an equivalent topology whose attribute values are most preferred by security experts?"**

Keywords- virtual network; security; 4Ward; MAVT

I. INTRODUCTION

Network virtualization is a concept in which virtualization technology is employed to achieve multiple independent networks over a common infrastructure substrate [1]. Virtual networks (VNets) are instantiated and managed independently of other virtual networks on the same infrastructure through various service provider models. Because they are isolated, VNets can employ communication protocols tailored to their service environment (that is, they do not necessarily have to use TCP/IP). These features lead to greater service provision flexibility than is currently enjoyed on today's Internet [2].

While greater flexibility is desirable, the introduction of network virtualization poses challenges from a trust and security perspective. Since multiple networks are sharing both node and link resources across multiple providers of unknown repute, it is natural for a client to wonder if the confidentiality, integrity, and availability of its data is secure. This is an open problem that is being actively investigated in the cloud computing paradigm where the security challenges are similar [3].

In this paper, we demonstrate a process for assessing the security posture of a VNet of arbitrary topology. We use Multi-Attribute Value Theory (MAVT) [4] to model the preferences of security experts with respect to security relevant attributes of VNet components. This model is used to develop a security assessment that represents a comparison between a new VNet topology and an equivalent topology whose attribute values are most preferred by security experts.

We present our security assessment process within the context of the network virtualization reference model developed by the 4WARD FP7 project [5]. This reference model provides the framework elements necessary to implement our process.

In Section II, we provide background information on the 4WARD FP7 virtualization reference model and introduce the foundational aspects of MAVT as they apply to our framework. In Section III, we introduce our VNet security assessment process and describe its component parts. In Section IV, we provide a concrete example of the application of our assessment process. In Section V, we elaborate on our process with respect to the example. In Section VI, we discuss related work and in Section VII we conclude with future work.

II. BACKGROUND

In this section, we describe VNet provisioning in the 4WARD FP7 framework and then briefly introduce Multi-Attribute Value Theory (MAVT) as it relates to our assessment process.

A. VNet Provisioning in the 4WARD FP7 Framework

VNets in the 4WARD FP7 project are composed using the business roles and framework elements shown in Fig. 1 [6]. A Service Provider (SP) expresses a need for a network with certain QoS or topology requirements (i.e. for IPTV, Gaming) and possibly custom routing and forwarding infrastructure. The SP works with a Virtual Network Provider (VNP) who interacts with a number of Physical Infrastructure Providers (PIPs) on its behalf. Each PIP owns and makes available a

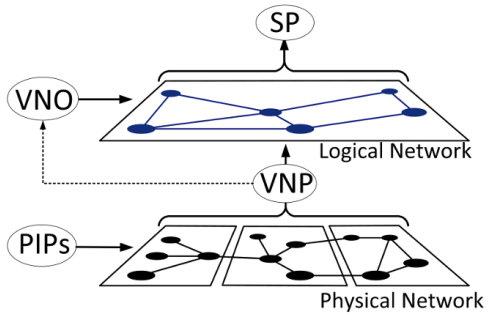

Figure 1. VNet Business Roles and Network Layers

978-1-4244-9538-2/11/$26.00©2011 IEEE

pool of node and link resources and has also established links with other PIPs. When the VNP finds a topology that matches the SP's needs (QoS, reachability, etc.), it works with each PIP to instantiate the topology and then passes management control to a Virtual Network Operator (VNO). The VNO installs the routing and forwarding software needed at each node and performs the other configuration tasks needed to make the SP operational.

From a security assessment perspective, a key phase of the VNet provisioning framework is *discovery*. Because the VNP cannot always know what capabilities each PIP can offer, the discovery phase allows the VNP to advertise its requirements and the PIPs to advertise their resources [7]. To facilitate discovery, a resource description framework is included as part of the 4WARD reference model [5]. Each network element in a PIP's inventory is described using a schema that allows for the annotation of functional and non-functional attributes. Fig. 2 (redrawn from [7]) illustrates the schema for a generalized network element of which node and link are sub-classes. Node attributes include *OS Type* and *Virtual Environment* while link attributes include *Link Type*, *Media Type*, etc. We view schema attributes from a security perspective and draw conclusions based on the security information they contain.

B. Multi-Attribute Value Theory

Our security assessment approach is an application of Multi-Criteria Decision Making (MCDM). With respect to various dimensions of security, we are looking for the "best" alternative (VNet topology) from a set of alternatives where each is defined by a unique set of values for certain important criteria (i.e. node and link attributes obtained during discovery). Our approach models the preferences of security experts with respect to schema attributes that are considered to have security implications. To build these preference models, we leverage the theoretical and axiomatic foundations of Multi-Attribute Value Theory (MAVT) which deals specifically with the modeling of preferences in complex decision scenarios.

In MAVT, individual preference behavior is modeled by a value function. For example, (1) shows a discrete value function for an individual's vehicle preference based on the manufacturer attribute.

$$\mathrm{v}_{\mathrm{car}}(x) = \begin{cases} 0.8, & x = \mathrm{Mazda} \\ 0.6, & x = \mathrm{GM} \\ 0.55, & x = \mathrm{Ford} \end{cases} \qquad (1)$$

When a decision is based on *multiple* attributes, then each combination of all possible values of each attribute is an alternative that a decision maker must consider. For example, if the multi-attribute problem was to select a "best car", then each alternative is a different combination of make, model, colour, etc. The traditional approach to modeling multi-attribute decision problems has been *synthesis* in which individual value functions are first created and then combined using an aggregation model [8]. In this paper, we use the additive aggregation model shown in (2) to construct multi-attribute value functions [4].

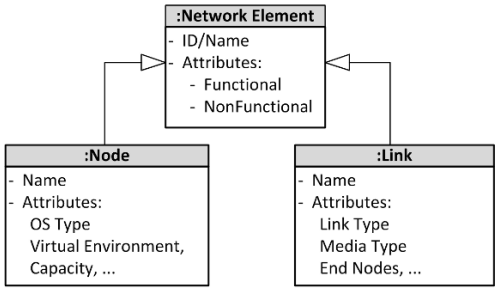

Figure 2. Resource Description Schema

$$\mathrm{v}(x) = \sum_{i=1}^{n} \alpha_i \mathrm{v}_i(x_i) \qquad (2)$$

Here, $\mathrm{v}_i(x_i)$ are single-attribute value functions scaled from 0 to 1 respectively and α_i are scaling constants with $\sum_{i=1}^{n} \alpha_i = 1$. The scaling constants are parameters introduced by the additive aggregation model and are used to define the relationship of each attribute with respect to the others [8]. Equation (2) is a simplification of the more general multiplicative form and is only valid under certain conditions [9]. These include demonstrating that the attributes of the problem space are either mutually difference independent or mutually preference independent [4].

III. Security Assessment Process

In this section, we describe our security assessment process which is divided into two parts. The first part involves developing a multi-attribute value function in the form of (2) for each type of VNet element (i.e. for nodes and links). In the second part, we combine these value functions into an aggregate model that we can use to assess arbitrary VNet topologies based on their specific values.

We describe the details of each part in the following sections and then present an example. Throughout this description, we make reference to *security expert* and *preference modeler* roles. Security experts provide the knowledge and experience upon which the assessment process is based. Preference modelers provide expertise in applying MAVT principles to the construction of the VNet security assessment model.

A. Multi-Attribute Value Function Modeling

In this part, we describe the four steps that we take to construct security preference models of each VNet network element. These steps include attribute selection, attribute independence testing, single- and multi-attribute value function development. The following subsections describe each step in more detail.

1) Attribute Selection: In this step, security experts examine all of the attributes that are used to describe each VNet element and select those that they consider to have some influence on the confidentiality, integrity, or availability dimensions of security. Table 1 shows examples of the node and link attributes that a security expert might consider relevant for each dimension of security. These attributes were

Table 1. Example Node and Link Attributes

Security Dimension	Link Attribute	Node Attribute
Confidentiality	VL: Virtual Link Type ET: Encryption type MT: Media type	VE: Virtual Environment OS: Operating System
Integrity	HA: Hash Algorithm PA: Peer Authentication	VE: Virtual Environment OS: Operating System
Availability	MT: Media type	VE: Virtual Environment OS: Operating System

drawn from those presented in [7] and extended to provide some added richness for demonstration purposes.

2) Attribute Independence Testing: The additive model in (2) will only be accurate if the attributes chosen by the security expert meet certain independence conditions. An experienced preference modeler will design and present a series of questions intended to validate attribute independence. For example, to establish the independence of the VE and OS attributes in Table 1 (for example, with respect to confidentiality), the preference modeler might begin by asking the security expert to consider his preference for Red Hat Linux versus Windows2K when both are hosted on a XEN virtual environment. The preference modeler would then ask the security expert to reconsider his preference for Red Hat Linux versus Windows2K when both are hosted on a VMWare virtual environment. If there is no change to his preference for Red Hat Linux versus Windows2K when the virtual environment changes, then support is gained for independence between VE and OS. After a series of such questions, mutual difference independence is either established for all attributes or it is not. In the latter case, it may be possible to render attributes independent through the creation of artificial attributes that are sums or differences of the dependent attributes (e.g. see [10]). At worst, dependent attributes can be combined to eliminate the dependencies. For example, if VE and OS were found to be dependent, then a third attribute could be created to represent every possible combination of VE and OS.

3) Single-Attribute Value Functions: Once difference independence is demonstrated, then each single attribute value function $v_i(x_i)$ in (2) can be developed independently while holding all other attributes at some arbitrary level [4]. This is the great advantage of the additive model and certainly justifies the effort invested in demonstrating attribute independence. Each single attribute value function captures the security expert's preferences for the values of that attribute along a given security dimension in a manner similar to (1). For example, the OS attribute can take discrete values whose domain includes all possible operating systems. Assuming that the only choices for OS were SELinux, BSD, and Win2K, then the preference function for OS (with respect to e.g. confidentiality) might resemble the following:

$$v_{\text{OS Conf}}(x) = \begin{cases} 0.75, & x = \text{SELinux} \\ 0.50, & x = \text{BSD} \\ 0.21, & x = \text{Win2K} \end{cases} \quad (3)$$

Each attribute may have up to three value functions – one for each of confidentiality, integrity, and availability. The applicability of each attribute to each security dimension is decided by the security experts during attribute selection.

4) Multi-Attribute Value Functions: Once all single-attribute value functions are determined, multi-attribute value function are created for each of confidentiality, integrity, and availability by determining appropriate scaling constants α_i in (2). The method of determining the scaling constants depends on the modeling approach taken. An example using MACBETH [12] is provided in Section IV.

B. Aggregate Model

The second part of the security assessment process is to develop an aggregation model that combines the multi-attribute value functions for each VNet node and link in a meaningful way. The aggregation model must also be invariant to the size or structure of the VNet so that comparisons between assessments are possible. We propose the following relatively simple aggregation model:

$$V_j = \{\bar{x}_j, \sigma_j, \text{Low}_j\}, \; j \in \{C, I, A\} \quad (4)$$

C, I, and A represent confidentiality, integrity, and availability respectively. The arithmetic mean $\bar{x}$ provides the average security value across the VNet and the standard deviation σ gives a measure of dispersion about this mean. The values of Low_j report on the lowest assessment for each dimension and are included to address a common concern that a system's overall security is only as strong as the weakest link [11].

Our aggregation model produces a security assessment in each dimension of security (for example, $V_C = \{\bar{x}_C, \sigma_C, \text{Low}_C\}$ for confidentiality). We consider it important to maintain separate assessments for each of confidentiality, integrity, and availability because each of these dimensions may have different importance to SPs.

IV. An Example

In this section, we provide a short example to demonstrate our assessment process. For context, we assume that an SP wants to provide a streaming media service and has engaged a VNP to provide a suitable VNet. However, the SP expresses a desire for some assurance that the confidentiality of its property will be preserved on the network. We assume that the VNP has selected a VNet topology that meets the client's functional and QoS requirements and must now compute a security assessment to manage the client's security concerns.

A. Value Function Construction

We begin by assuming that a preference modeler is assisting with this effort and has already facilitated the selection of the security relevant attributes as shown in Table 1. We assume that mutual difference independence between these attributes has also been established. Several security

Table 2. Attribute Categories and Values Determined by Security Experts for a Subset of Security Relevant Attributes

Attribute	Category	Values
Node Virtualization Environment (VE)	Separate Machines	None
	Type I VMM	VMWare ESX, XEN, …
	Type II VMM	VMWare WS, KVM, …
	OS VMM	UML, BSD Jails, …
	Process VMM	Bochs, QEMU, …
Link Media Type	Fiber	Any
	Twisted Pair	UTP, STP, …
	Coaxial Cable	RG-8, RG-58, …
	Wireless	XBee, 802.1X
Link Encryption	None	AES_CBC_2048
		3DES_CBC_2048
		RC5_CBC_56, …
		None

experts who are working for the VNP are assisting with the development of the security value models.

The first task for the experts is to identify the sets of values that each attribute in Table 1 can assume. Table 2 shows several examples of specific attribute values. Note that several attributes in Table 2 have been subdivided into categories for generalization purposes. For example, Link Media Type (MT) is subdivided into Fiber, Coax, Twisted Pair and Wireless categories. This technique allows the preference modeling exercise to be performed with possibly incomplete information about all of the specific values that are likely to be encountered. For some attributes (such as Link Encryption), the set of possibilities is reasonably well bounded so no categories are necessary.

Next, the preference modeler facilitates the development of a single-attribute preference function for each attribute. In our example, the preference modeler uses MACBETH [12] as a preference modeling process and the M-MACBETH [13] tool to capture and process modeling artifacts. Fig. 3 illustrates an

Figure 3. M-MACBETH Judgement Matrix for Media Type Confidentiality

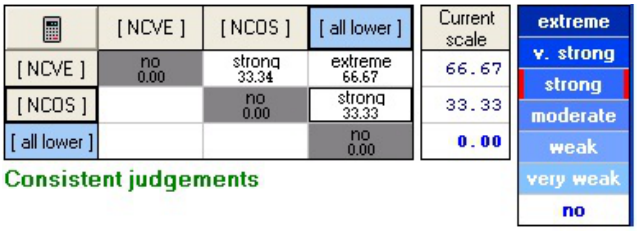

Figure 4. M-MACBETH Judgement Matrix for Scaling Constants

attribute value judgment table computed using M-MACBETH for the attribute Media Type (MT) with respect to confidentiality. When all judgements in this table are complete and there are no inconsistencies, the "Current Scale" column represents the discrete preference function for the MT attribute. A similar exercise is performed for each attribute in each security dimension. The preference functions for each attribute in this example is shown in Table 3.

Once all of the single-attribute value functions have been computed, the preference modeler uses M-MACBETH again to derive the scaling constants needed to construct the multi-attribute value function for each network element. An example of the elicitation of scaling constants using M-MACBETH is shown in Fig. 4. On the axes, "NC" represents node confidentiality while "VE" and "OS" are the Virtualization

Table 3. Preference Function Values for VNet Attributes

Node Confidentiality, Integrity, Availability	Virtual Environment	i	Separate Computers	Type I VMM	Type II VMM	OS VMM	ProcessVM
		$v_{VE}(i)$	1.00	0.81	0.55	0.28	0.00
	Operating System	i	µK, Open Src	µK, Closed Src	MonoK Open Src	MonoK Closed Src	Unknown
		$v_{OS}(i)$	1.00	0.70	0.40	0.28	0.00
Link Confidentiality	Encryption Type	i	AES_CBC_2048	3DES_CBC_2048	AES_CBC_1024	3DES_CBC_1024	Others
		$v_{ET}(i)$	1.00	0.95	0.72	0.69	0.00
	Media Type	i	Fibre	Coaxial Cable	Twisted Pair	Wireless	
		$v_{MT}(i)$	1.00	0.75	0.48	0	
	Virtual Link Technology	i	Physical Separation	Logical Separation	No Separation		
		$v_{VL}(i)$	1.00	0.45	0		
Link Integrity	Peer Authentication	i	HW_Cert	SW_Cert	Keyed_Mac	None	
		$v_{PA}(i)$	1.00	0.65	0.42	0	
	Hash Algorithm	i	SHA512	RIPEMD128	MD5	None	
		$v_{HA}(i)$	1	0.80	0.35	0	
Link Availability	Media Type	i	Fibre	Coaxial Cable	Twisted Pair	Wireless	
		$v_{MT}(i)$	1.00	0.90	0.70	0.00	

Table 4. Multi-Attribute Value Functions for Node and Link Elements With Respect to for Confidentiality, Integrity, and Availability

Link Value Functions	
Confidentiality	$V_{CL\,i} = 0.60v_{ET}(i) + 0.15v_{MT}(i) + 0.25v_{VL}(i)$
Integrity	$V_{IL\,i} = 0.69v_{PA}(i) + 0.31v_{HA}(i)$
Availability	$V_{AL\,i} = v_{MTA}(i)$
Node Value Functions	
Confidentiality	$V_{CN\,i} = 0.67v_{VE}(i) + 0.33v_{OS}(i)$
Integrity	$V_{IN\,i} = 0.67v_{VE}(i) + 0.33v_{OS}(i)$
Availability	$V_{AN\,i} = 0.67v_{VE}(i) + 0.33v_{OS}(i)$

Environment and Operating System attributes respectively. The "Current Scale" column of Fig. 4 represents the scaling constants for node elements with respect to confidentiality. The final multi-attribute value functions are shown in Table 4. There is a multi-attribute value function for each of confidentiality, integrity, and availability for both nodes and links. The node value functions are the same for each security dimension because the security experts considered the VE and OS attributes to have an equivalent influence across all three.

B. Security Assessment of the VNet

Fig. 5 shows an example VNet topology that the VNP might have developed to satisfy the SP's requirements. Table 5 shows the specific attribute values for each network element given the proposed topology in Fig. 5. Using Tables 3 and 5, values for each network element in Table 4 can be computed. The results are used with our aggregation model in (4) to produce the results summarized in Table 6.

V. DISCUSSION

The mean and standard deviation in Table 6 provide a useful metric for establishing the extent to which security is balanced across the VNet. For example, the Low value for link confidentiality (0.11) does not compare well to the average (0.72). If we recall that the SP had concerns about the confidentiality of its property on the VNet, then this low value might be of significance. Thus, the VNP and SP can focus

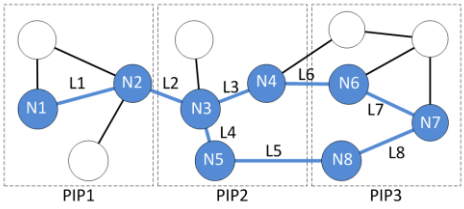

Figure 5. Example Virtual Network Topology

Table 6. Aggregate Security Assessment Model Results

Security Dimension	Link			Node		
	$\bar{x}$	σ_n	Low	$\bar{x}$	σ_n	Low
Confidentiality	0.72	0.27	0.11	0.59	0.19	0.33
Integrity	0.64	0.17	0.29	0.59	0.19	0.33
Availability	0.79	0.33	0.67	0.59	0.19	0.33

their limited energies on addressing this problem with the aim of bringing the value up to the average instead of being distracted by areas that are already sufficiently secure. Although our assessment process is fundamentally descriptive, there may nonetheless be some limited opportunities for adjustment prior to committing to a topology. One alternative would be to negotiate with the PIP(s) in question (through the VNP) to raise the security level of the problematic element (especially if the PIP is the only one offering service to a geographic region). Another alternative would be to conduct a threat and risk assessment in the area of the weak element to identify the existence of compensating controls. This is where access to node and link attributes that are not security related can be of significant use. For example, geographical location attributes might indicate that the potential for either casual or deliberate eavesdropping on the link is low resulting in no requirement to adjust the VNet. Alternatively, local attribute information might indicate a risk higher than the SP is willing to accept resulting in a requirement for the SP and VNP to negotiate a change

It is important to emphasize that the results shown in Table 6 do not *guarantee* security nor do they provide an absolute measure of security. Rather, they provide a benchmark that can be used to measure the extent to which the VNet compares to one whose attribute values would have been chosen by security experts had security been the only design consideration. These results answer the question "how well does my VNet compare to the experts?" as opposed to "how secure is my network?" A similar but much less formalized approach is taken each time a network diagram is passed to a security expert for review and comment. His or her assessment is security-centric and is based on what the expert knows at the time.

VI. RELATED WORK

The authors of [14] describe a method in which security protocols are automatically selected based on the use of Multi-Attribute Utility Theory (MAUT) in order to balance the opposing demands of security, energy consumption, and QoS in the specific context of link security protocol selection. The

Table 5. Node and Link Attribute Values for the VNet in Fig. 5

Node Attributes			Link Attributes					
Node	**VE**	**OS**	**Link**	**ET**	**MT**	**VL**	**PA**	**HA**
N1	UML	Linux	**L1**	None	802.11	VLAN	Keyed Mac	None
N2	UML	Linux	**L2**	3DES_CBC_1024	Fiber	MPLS	Keyed Mac	SHA256
N3	ESX	Win2K	**L3**	3DES_CBC_1024	TP	VLAN	Keyed Mac	RIPEMD
N4	ESX	Win2K	**L4**	3DES_CBC_1024	TP	VLAN	Keyed Mac	RIPEMD
N5	ESX	Win2K	**L5**	AES_CBC_2048	Fiber	TDM	Software Cert	SHA256
N6	XEN	L4	**L6**	AES_CBC_2048	Fiber	TDM	Software Cert	SHA256
N7	XEN	L4	**L7**	3DES_CBC_2048	Fiber	VLAN	Hardware Cert	MD5
N8	XEN	L4	**L8**	3DES_CBC_2048	Fiber	VLAN	Hardware Cert	MD5

notion of using MUAT to optimize alternatives based on aspects of both security and QoS is similarly applied in [15]. We found the concepts presented in [14] and [15] intriguing and extend them in this paper. We generalize the application of multi-attribute decision theory to the problem of security assessment on a composite Virtual Network as a whole. At the same time, we took a more rigorous approach towards the application of decision theory by focusing on the theoretical underpinnings of multi-attribute utility and value theory. Our approach addressed key modeling constraints that were not well described in either [14] or [15].

In [16] and [17], the Analytic Hierarchical Process/Dempster-Shafer Evidence Theory (AHP/DS) is applied to system security risk assessment. AHP is an alternative approach that can be used in Multi-Criteria Decision Making to perform relative measurement of criteria [18]. However, the authors focus on using the AHP/DS in the context of traditional risk assessment in typical network environments (i.e. not VNets) which requires the integration of threat, impact and probability judgments to achieve a result. We focus only on security value which allows us to consider threat, impact, and quality of service as separate concerns.

VII. Conclusion and Future Work

One area of our assessment process that could use further attention is the issue of model development using multiple experts. Clearly, using more than one expert is desirable from a diversity perspective. However, MACBETH was designed to work with one set of preference values. Multiple experts would need to work in a group setting and achieve consensus which can be a challenging task in its own right. One possible solution would be to apply Dempster-Schafer (DS) evidence theory in a manner similar to [19] in order to obtain and combine independent assessments from individual security experts. The Analytical Hierarchal Process (AHP) has already been extended in this manner and MACBETH might benefit from the same consideration.

We assume that assessment is finished when the VNet is handed over to the VNO for operations. However, there are many good reasons for the physical infrastructure beneath the logical VNet to be in a constant state of flux (e.g. maintenance, load-balancing, path optimization). Therefore, work remains to determine when security *reassessment* needs to be performed and what policy actions are invoked when the results are unexpected.

Finally, our security assessment process is descriptive; it relies on accurate and honest reporting of node and link attributes by infrastructure providers. Clearly, there will be incentive for misrepresentation if the economic benefits are large enough. A more *prescriptive* methodology would *require* certain attributes to be reported and, in addition, provide evidence of the values claimed. By providing evidence to bolster claims, it is possible to address security *assurance* which is a dimension of security that is often overlooked. Assurance provides evidence of the *correct design and functioning* of a security mechanism and is one conceptual step ahead of simple compliance auditing.

References

[1] J. Carapinha and J. Jiménez, "Network virtualization: a view from the bottom," in *Proceedings of the 1st ACM workshop on Virtualized infrastructure systems and architectures*, pp. 73–80, 2009.

[2] N. Feamster, L. Gao, and J. Rexford, "How to lease the internet in your spare time," SIGCOMM Comput. Commun. Rev., vol. 37, no. 1, pp. 61-64, 2007.

[3] K. Popovic and Z. Hocenski, "Cloud computing security issues and challenges," in MIPRO, 2010 Proceedings of the 33rd International Convention, pp. 344 -349, 2010.

[4] J. Figueira, S. Greco, M. Ehrogott, and J. Dyer, "Maut — Multiattribute Utility Theory," in *Multiple Criteria Decision Analysis: State of the Art Surveys*, vol. 78, Springer New York, 2005, pp. 265-292.

[5] P. A.A. Gutierrez, et al., "D-2.3.1 Final Architectural Framework," 4Ward Project. 216041, Revision 1.0, 10 June 2010. Available: www.4ward-project.eu.

[6] L. Mathy, G. Schaffrath, C. Werle, P. Papadimitriou, A. Feldmann, R. Bless, A. Greenhalgh, A. Wundsam, M. Kind, and O. Maennel, "Network virtualization architecture: proposal and initial prototype," Barcelona, Spain: ACM, 2009, pp. 63-72.

[7] I. Houidi, W. Louati, D. Zeghlache, and S. Baucke, "Virtual Resource Description and Clustering for Virtual Network Discovery," Communications Workshops, 2009. ICC Workshops 2009. IEEE International Conference on, 2009, pp. 1 -6.

[8] J. Figueira, S. Greco, M. Ehrogott, and B. Roy, "Paradigms and Challenges," in Multiple Criteria Decision Analysis: State of the Art Surveys, vol. 78, Springer New York, 2005, pp. 3-24.

[9] R.L. Keeney and H. Raiffa. Decision with Multiple Objectives: Preference and Value Tradeoffs. Cambridge University Press, New York, 1993.

[10] P. Farquhar and L. Keller, "Preference intensity measurement," *Annals of Operations Research*, vol. 19, pp. 205-217, 1989.

[11] K. Julisch, "Security compliance: the next frontier in security research," in Proceedings of the 2008 workshop on New security paradigms, pp. 71-74, 2008.

[12] C. A. B. E. Costa and M. P. Chagas, "A career choice problem: An example of how to use MACBETH to build a quantitative value model based on qualitative value judgments," *European Journal of Operational Research*, vol. 153, no. 2, pp. 323 - 331, 2004.

[13] www.m-macbeth.com

[14] L. Volker, C. Werle, and M. Zitterbart, "Decision process for automated selection of security protocols," in *Local Computer Networks, 2008. LCN 2008. 33rd IEEE Conference on*, pp. 223 -229, 2008.

[15] M. Alia and M. Lacoste, "A QoS and Security Adaptation Model for Autonomic Pervasive Systems," Computer Software and Applications, 2008. COMPSAC '08. 32nd Annual IEEE International, 2008, pp. 943 - 948.

[16] Y. Qing, Z. Changhong, W. Xiaoping, and Z. Dingjun, "Information Security Risk Assessment Based on AHP/DST," in Management and Service Science, 2009. MASS '09. International Conference on, pp. 1 -4, 2009.

[17] L. Simei, Z. Jianlin, S. Hao, and L. Liming, "Security Risk Assessment Model Based on AHP/D-S Evidence Theory," in Information Technology and Applications, 2009. IFITA '09. International Forum on, vol. 2, pp. 530 -534, 2009.

[18] M. Beynon, B. Curry, and P. Morgan, "The Dempster-Shafer theory of evidence: an alternative approach to multicriteria decision modelling," Omega, vol. 28, no. 1, pp. 37 - 50, 2000.

[19] X. Cuihua and L. Jiajun, "An Object-Oriented Information System Security Evaluation Method Based on Security Level Distinguishing Model," in Web Information Systems and Mining, 2009. WISM 2009. International Conference on, pp. 497 -500, 2009.