Proceedings of the International Multiconference on
Computer Science and Information Technology, pp. 79 – 82

ISBN 978-83-60810-14-9
ISSN 1896-7094

USERING. Educational Self-Tuning–Recommendations in the 8th Level of ISO/OSI Model

Miroslaw Bedzak
Institute of Control Engineering
Szczecin University
of Technology,
ul. Sikorskiego 37,
Poland
Email: bedzak@ps.pl

***Abstract*—It is autumn 2012…The VMware Infrastructure …3, 4 editions virtualised crucial components of IT environment, i.e. computing (CPU, RAM), networking and storage. However, an important element was overlooked. Which one? A user. There was no mechanism built in into VI3/VI4 that would support administrator in gaining effectively the skills of implementing solutions advised by manufacturer, the so-called recommendations ("best practice", etc.). Either, the high level of user's skills (primarily, administrator's ones) were not treated as a valuable resource of LAN infrastructure that could be (should be) used, while a "surplus" could be virtualised for a common good of the society (local and/or global), concentrated around the enterprise-class infrastructure virtualisation technology. The latest edition, VI5 beta, brings also an important change in this respect in the form of a new module, VMware Usering, which is directed in the current version (i.e. beta version) first of all towards security hardening, i.e. the linguistic inference has been accomplished by a method of fuzzy control basing on the knowledge-base built on the recommendation of VI5 beta manufacturer. The VMware Usering is a set of tools, stimulating users to take up actions being consistent with manufacturer's recommendations (VMware User Hardening) and virtualising (optionally for administrators with HIGH FUZZY rating) the competence resource of advanced users (VMware User Competence Sharing). The rise of a resistance level of IT infrastructure to increasing threats of internet security is also a manufacturer's own interest, therefore one can expect in the near future a popularisation of VMware Usering-class solutions as an important tool supporting an average internet surfer in his/her solitary struggle against crackers at the level of 8th OSI model layer** .

I. Introduction

IT IS autumn 2015… Computer software is not only a code with specific functionality. It is also – and perhaps first of all – a knowledge, experience and competences of computer programmers enclosed (also outside the code) in a set of the so-called recommendations. Owing to them, a user can avoid obstacles and traps of the interference of tens (hundreds) of options (chances) "at choice". Obviously, a user can but does not have to… The tandem of software functionality and user competence (including the use of recommendations) determines at last the quality of IT solution.

Apart from controlling and managing a specific functionality of IT system, an important issue (in present-day internet times) is to pay due attention (at least 10% of daily work time with IT system?) to IT security questions. Besides implementing hardware and software solutions, a key element is the quality of the weakest link, i.e. the quality of knowledge and user competence.

Probably the IT infrastructure that works on-line with the Internet is helpless (except for entries in system logs) when administrator has turned off (perhaps unintentionally) its protecting systems, i.e. firewall/IDS/IPS (exposing the same its resources to the prey of crackers). With some exaggeration, we can probably describe the past IT systems as "deaf-mute" ones, i.e. helpless on the one hand "to admin insanity/ignorance", while not using completely the experience and professionalism of brilliant user (administrator) on the other hand. There was no feedback in them: "reprimand for making and sticking to an error" and first of all rewarding "good behaviour consistent with manufacture's recommendations" [1]-[3].

Two extremely popular previous versions, VI3 and VI4, virtualised crucial hardware and software components of IT infrastructure, forgetting however about a key link (for its proper functioning), i.e. about a user.

Together with VI5 beta Enterprise, we are receiving a tool, VMware Usering, stimulating (supporting intensively) a user for taking up actions that are consistent with manufacturer's recommendations, i.e. VMware User Hardening (VMware UH) as well as a tool virtualising the competence resource (of advanced users with f(UR):= HIGH rating), i.e. VMware User Competence Sharing (VMware UCS).

II. Usering Security, or Educational Self —Tuning in the 8th Layer of OSI Model.

A. Admin in the "open loop" of acquiring competence/ knowledge/ experience.

The detailed discussion of VMware Usering mechanism surpasses the frames of the present paper. It is sure enough that descriptions referring to most new mechanisms available in VI5 edition will show in the near future. Below, only the essence of VMware UH and VMware UCS operation will be

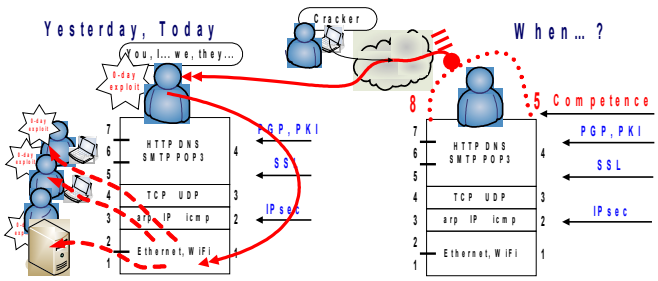

Fig 1 . User Hardening, a tool supporting the user in counteracting internet attacks from the 8th layer of OSI model: Competence layer.

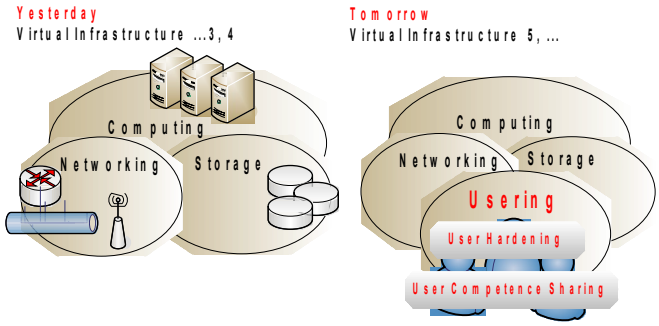

Fig 2. Usering, next virtualized component of the enterprise-class IT environment.

illustrated on selected examples. Not many users have knowledge of availability of VMware UH also for older editions of Virtual Infrastructure 3 and 4 (after installing additionally manufacture's patches to Virtual Center server ver. 2 or 3). In the present version (i.e. VI5 beta), VMware UH is using manufacturer's recommendations that are connected with IT security hardening, i.e. Vmware UH.

Until recently, almost all of us have accepted quietly a common practice that responsibility of admin is to "become" (of a sudden the best) or "becoming" an expert (at last after many months /sometimes many years) (No 1 problem), who will be able, apart from managing classic IT resources, to "keep a tight rein on" (meaning: extend knowledge of) a common user of virtual infrastructure.

The no 1 problem is a process (frequently long-lasting one) of coming in admin competence to the knowledge level of software engineers (authors) (VMware team): from studying "case study"/"best practice" "helps" /pdf files/ through specialist courses to own experience/experimenting with test/ production network. Direct contact/exchange of experience (meaning: sharing with each other) between computer programmer/software engineer (author) and a user/administrator has been out of question (apart from a small group using Help Line). Out of hundreds / thousands of documentation pages, few users "shell out" most important procedures, primarily those advised by manufacturer, i.e. recommendations. And what is the effect of this?

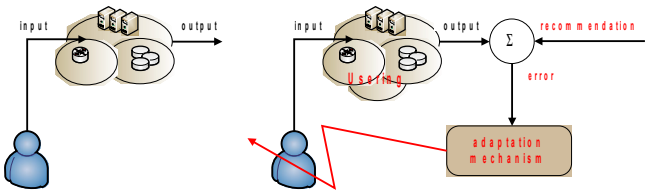

Fig 3. User in the "opened (left)/ closed (right) loop", or educational self-tuning.

The IT system has quietly permitted sometimes to "demolish" itself, or sometimes to "tune up perfectly", depending on admin competence. A common practice, used also by a manufacturer, was to record important events (unfortunately) in many scattered logs/data-bases. Every admin will admit that effective daily tracking (and first of all correlating any number) of tens/hundreds/thousands of scattered events is almost impossible with the quality comparable at least to solutions of Intrusion Detection/Prevention System type. The process described above can be summarised unfortunately as "admin all alone in the open loop of acquiring knowledge":

- lack of built-in mechanism that evaluates *on-line* and *on-time* the conformity of user actions (including admin) with the advised manufacturer's recommendations, e.g. admin can of course do "everything, but it will be good if he/she does not take up actions that decrease the system security, does it?
- lack of mechanism (rewarding/promoting one) that uses user competence and acquired knowledge for the good of local/global user society concentrated around a specific technology (except for enterprise discussion lists),
- similarly to counteracting the waste of resources of the non-virtualised server computing type, we all agree with the thesis that one can counteract with equal determination the waste of acquired knowledge and competence of professional users.

B. Admin in the "closed loop", or educational self-tuning.

When closing feedback loops, we receive immediately profits:

- administrator sees "without delay" the effect of his/ her actions (choices of options, configurations, activation/deactivation…, etc.) on "educational self-tuning error" (minimum one the best) with respect to advised manufacturer's recommendations,
- evaluation of "educational self-tuning error" (difference between user choice/decision and manufacturer's recommendation) is made (in the present version, i.e. VI5 beta) with fuzzy logic method: except for interference of the "black-white" type, i.e. zero/"no conformity"/"maximum error" vs. one/"100% conformity"/"zero-value error", we are using affiliation degrees (set of real numbers within a range of ≤ 0; $1 \geq$) for a fuzzy set that represents one of the values of linguistic variable *competence* { *Low, Medium, High* }:

error of educational self-tuning $_{FUZZY}$:= recommendations of manufacturer $_{FUZZY}$ – decisions of administrator $_{FUZZY}$

- apart from the c onformity with important manufacturer's recommendations, one can evaluate "educational self-tuning error" for a common user who, when acting within authorisations (permissions), i.e. making use of trappings (privilege) attributed to his/her part (role), can be "rewarded with a neutral mark or higher f (UH)" for "moving" inside the cage determined by the role" and "punished with a neutral mark or lower f (UH)" even for taking up "only attempts" to make use of privileges not attributed to his/her role".

C. *VMware User Hardening* $_{security}$ *(VMware UH* $_{security}$ *).*

Abstract he mechanism that allows for closing the educational loop of feedback is just VMware UH module (apart from VMotion, VMware HA, VMware DRS and two other novelties in VI5 beta version, it is the next option for Standard and Enterprise versions requiring the licence). In VMware UH, the interference has been accomplished by a method of fuzzy control (computational intelligence), basing on the knowledge-base constructed on manufacturer's recommendations [6],[7].

UH $_{security}$: User Hardening $_{security}$

$e_{FUZZY} \cong r_{FUZZY} - d_{FUZZY}$

- e $\{e_1, e_2 \ldots e_n\}$- error of educational self-tuning
- r $\{r_1, r_2 \ldots r_n\}$ - recommendations of manufacturer
- d $\{d_1, d_2 \ldots d_n\}$ - decisions of administrator
- f (UH):= { LOW_{FUZZY} , $MEDIUM_{FUZZY}$, $HIGH_{FUZZY}$ }
- Objective: local evaluation (automatically and without delay) of administrator's (user's) implementation of recommendations (of manufacturer)

The key element of fuzzy control is expert knowledge-base constructed on manufacturer's recommendations:

(+) It is recommended…

(-) VMware does not recommend using…

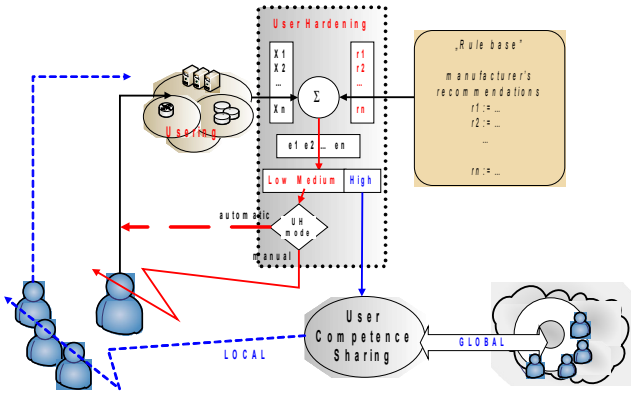

Fig 4. Concept of using computational intelligence in the "closed loop" of educational self-tuning of User Hardening module-tuning.

written in the form of (IF… Then…) rules

IF *premiss1* AND *premiss2* AND…

Then *conclusion1* AND *conclusion2* …

that use the values of linguistic variable fuzzy logic described by means of appropriate fuzzy sets. The VMware UH does not analyse "every step" of user; it take into account only these actions, for which a manufacturer's recommendation exists in the knowledge-base. In the supplement Appendix, the examples of manufacturer's recommendations are given (scattered in rich documentation) that increase the IT security of infrastructure with respect to its crucial components: ESX Server Host, Service Console, Virtual Machine and VirtualCenter.

In order to illustrate the essence of VMware UH $_{security}$ operation, we will use the first recommendation from the Appendix that refers to ESX installation and evaluate a possible "educational self-tuning error", taking into account:

- default setting of manufacturer,
- decisions of administrator,
- recommendations of manufacturer,

hat is:

- error of educational self-tuning $_{FUZZY}$:= recommendations of manufacturer $_{FUZZY}$ - – decisions of administrator $_{FUZZY}$

f (UH):= $HIGH_{FUZZY}$

What does it mean in reality? As early as a few minutes of ESX 3 installation, administrator should "brake down" default settings (but not recommended by VMware!) in case of production environment (and not a test one) in order to ensure HIGHER security and aim at f (UH):= $HIGH_{FUZZY}$ mark [4], [5] :

- default setting "Create a default network for virtual machines" is not recommended for production environment by VMware manufacturer.

„ […] If the "Create a default network for virtual machines" is selected, virtual machine network traffic will share this adapter with the service console. This is not a recommended configuration for security purposes"

Conclusion:

- as early as a few minutes of administrator contact with infrastructure software, we can evaluate a probable

- error of educational self-tuning $_{FUZZY}$:= recommendations of manufacturer $_{FUZZY}$ – decisions of administrator $_{FUZZY}$

and interfere according to fuzzy control nomenclature about evaluating admin competence of the type:

- increase
- neutral
- decrease

receiving, e.g.:

μ (LOW FUZZY):= 0.0; μ (MEDIUM FUZZY):= 0.2;

μ (HIGH FUZZ):= 0.8 $\Rightarrow$:→ (UH):= 82% HIGH FUZZY

D. *VMware UH* $_{security}$ *: manual – automatic (autopilot) mode.*

The VMware UH $_{security}$ (in VI5 beta version) default operation mode is *manual* , i.e. presenting the error of educational self-tuning (with indication to recommended options) without enforcing choices/decisions/methods of user action consistent with manufacturer's recommendations. An interesting mode is *automatic* , which for the profile of VMware UH $_{security}$ edition, as a *security hardening* , will approve

(similarly to the *transaction* mechanism in the data-base nomenclature) only these decisions of user, which will not decrease (but rather increase) the global level of infrastructure security for production network.

III. VMware User Comptetence Sharing (UCS)

Natural consequence of minimising the error of educational self-tuning $_{FUZZY}$ of the competence resource for a specific user of VMware UH module at a respectively high level (e.g. over 75%) HIGH $_{FUZZY}$ is to move to next stage on the way to full Usering, i.e. to virtualise the competence resource of advanced users with VMware UCS module by "sharing"/"participation" for the good of local and/or global user society. The idea of VMware UCS functioning is springing from the mechanism of self-education of professional internet discussion list users. A particularly good example is the mechanism that supports evaluation of the importance/quality of post contents of the moderated discussion list VMWare VMTN Discussion Forums...Novice, Expert, Champion, and Guru. The VMware UH $_{security}$ fulfills a similar role to a moderator and opinions of internet surfers, but at a local level in evaluating the practical competence of a user who manages the advanced infrastructure.

VMware UCS uses of course a VMware UH $_{security}$ filter :

VMware UH $_{security}$: *filter_HIGH* {user1_ *LOW* , user2_ *HIGH* , … userN_ *MEDIUM* }= user2 and can work in the following modes (different possibilities are tested in the present beta version; final VMware UCS operation modes should be determined within the nearest months after all test are concluded):

- Local_info: users indicated by user2 (all, selected,…) will be familiarised with the current ranking of VMware UH $_{security}$ evaluation,
- Local_sharing: during taking up actions that are inconsistent with manufacturer's recommendations, a user has to receive a counter-signature from the user with HIGH mark,
- Global _sharing: a user2 user with HIGH mark receives a possibility/invitation from VMware manufacturer for co-operation for the good of the society concentrated around the product (its scope and form is determined by manufacturer).

IV. Conclusion

Internet surfers should be equipped with knowledge and competence that allow on the one hand for effective acquiring of advanced skills for daily management of (work with) modern IT systems, while enable counteracting against misuses from the part of less or more organised groups of internet crackers on the other hand. Because quick achievement of the aforesaid objectives is important for the well-comprehended business-like own interest of manufacturer, thus we can expect in the near future a popularisation of solutions of the VMware Usering class as an important tool that supports, among others, an average internet surfer in his/her alone struggle with crackers at a level of the 8th layer of OSI model. Undoubtedly, the strength of this solution lies in the skilful connection of a tool set that stimulates users for taking up actions, which are consistent with recommendations of VMware UH manufacturer and (optionally for administrators with $f(UH) := HIGH_{FUZZY}$ mark) virtualising the competence resource of VMware UCS users.

Appendix

Examples of manufacturer's recommendations that increase IT security of infrastructure with respect to its crucial components [8]-[11].

ESX Server Host:

Do Not Create a Default Port Group
Use a Dedicated, Isolated Network for VMotion and iSCSI
VMware best practices recommend that the service console and VMotion have their own networks for security reasons
Do Not Use Promiscuous Mode on Network Interfaces
Protect against MAC Address Spoofing (MAC address changes, Forged transmissions)
Secure the ESX Server Console
Mask and Zone SAN Resources Appropriately
Protect against the Root File System Filling Up

VirtualCenter:

Manually changing Most Recently Used to Fixed is not recommended. The system sets this policy for those arrays that require it. For active/passive storage devices, Most Recently Used is highly recommended
Comparing Raw Device Mapping to Other Means of SCSI Device
Virtual Machine
Disable Unnecessary or Superfluous Functions
Limit Data Flow from the Virtual Machine to the ESX Server Host
Isolate Virtual Machine Networks
Minimize use of the VI Console

Service Console:

Isolate the Management Network
Configure the Firewall for Maximum Security
Use VI Client and VirtualCenter to Administer the Hosts Instead of Service Console
Use a Directory Service for Authentication
Strictly Control Root Privileges
Limiting Access to su. Using sudo
Establish a Password Policy for Local User Accounts
Limit the Software and Services Running in the Service Console
Do Not Manage the Service Console as a Linux Host
Establish and Maintain File System Integrity
Maintain Proper Logging

References

[1] R. J. Anderson, "Security Engineering: A guide to building dependable distributed systems," 2001, Wiley & Sons.
[2] N. Ferguson and B. Schneier, "Practical Cryptography," Wiley & Sons, 2003.
[3] N. F. Johnson and S. Sushil Jajodia, "Steganography: Seeing the Unseen," IEEE Computer, 1998, February, 26-34.
[4] C. Chaubal: Security Design of the VMware Infrastructure 3 Architecture, VMware, 2007.
[5] C. Chaubal: VMware Infrastructure 3. Security Hardening, VMware, 2007.
[6] L. A. Zadeh, "From computing with numbers to computing with words–from manipulation of measurements to manipulation of perceptions". IEEE Trans. on Circuits and Systems–I: Fundamental Theory and Applications, vol. 45, no. 1, pp. 105-119, 1999
[7] L. A. Zadeh, "Web Intelligence, World Knowledge and Fuzzy Logic– The Concept of Web IQ (WIQ)", University of California Berkeley, 2004.
[8] VMware Infrastructure 3: Install and Configure. Laboratory Exercise, VMware, EDU-IC-3020-SL-B, 2006
[9] www.vmware.com/vmtn/resources/410, VMware Infrastructure 3 Architecture.
[10] www.vmware.com/pdf/vi3_installation_guide.pdf, Installation and Upgrade Guide.
[11] www.vmware.com/pdf/vi3_server_config.pdf, Server Configuration Guide.