SECURITY OF FUTURE SMART HOMES. CYBER-PHYSICAL THREATS IDENTIFICATION PERSPECTIVES

Zlatogor Minchev[1], Luben Boyanov[1] & Stiliyan Georgiev [2, 3]

E-mails: zlatogor@bas.bg, lb@acad.bg, stilliyan@gmail.com

[1] Institute of Information and Communication Technologies – BAS, Sofia, Bulgaria
[2] IMSETHC – BAS, Sofia, Bulgaria
[3] VISENSI Ltd., Sofia, Bulgaria

Abstract: *The paper is discussing security threats identification perspectives in modern smart homes modeled as cyber-physical systems that encompass technologies, human factors, their activities and specifics. Generally, the modeling process is performed with the help of Entity-Relationship representation, combined with experts' knowledge in an own ad-hoc software environment. The obtained results give a possibility for building a scenario context and further more detailed threats analysis that could be transformed with the agent-based paradigm into an automated smart homes security system.*

I. Introduction

In todays' world the digital society is already an indispensible part of our everyday life. The modern understanding of smart devices together with fast progressing web technologies has already entered our work, homes and even cities [1], [2]. According to some very recent studies [3], [4], [5] the trends for 2013 Internet technologies are basically related to Web 2.0 and Web 3.0 ideas about information sharing, social networks with direct access from different smart devices (smart phones, tablets, TVs, watches, etc.). These, however are opening the vast cyber security problem area together with the role of the human factor.

Generally, the topic could also be addressed to cyber-physical systems field [6] and is really producing an interesting area for research, putting together technologies and human interaction in a rather broad context. An important note here is also related to the upcoming Web 4.0 and Web 5.0 encompassing an embedded and improved artificial intelligence based sensors and robots that will have an augmented set of rights and permissions for own self-activities.

A practical projection, related to this progress, is directly observable in modern smart homes that offer their inhabitants a number of useful automated smart services, e.g.: the ability for remote access to your air conditioner, home light systems, household machines, and going further through house cleaning, alarming systems, or even further – home entertainments (noting the interactive television and the new multidimensional virtual realities trends), robots companions and assistants. In today's digital era the smart homes are already addressing integration in smart cities with drone reconnaissance systems, smart art installations, shops, etc.

This briefly outlines the large problem field for cyber-physical systems exploration, which are already everywhere in our daily life.

Further on, in the present work the cyber-physical security study perspectives, concerning future smart homes will be considered from a methodological view point, encompassing threats identification.

II. Methodological Framework

Generally, the identification of cyber threats is a complex process and here it is focused around the smart homes problem, assuming the idea for smart homes consideration as cyber-physical systems that include technologies and human factors with their activities and specificities. Being complex enough this explanation could be easily translated into the model world through the utilization of experts' knowledge and morphological analysis [7]. The basic idea here is to extract the key directions and facets for studying the problem with the experts' knowledge support and to produce a context set for a number of human factor activities.

As far as this process evidently requires present and future beliefs implementation the context is used to be reckoned as 'plausible future' and the building elements 'scenarios' that encompass different mutually exclusive 'alternatives' ($A_{i,j}$, $i = 1,\ldots,n$, $j = 1, \ldots, m_i$; n – number of dimensions, m_i – number of alternatives for the i-th dimension; $n, m \in \mathbf{N}$) from a multiple n key 'dimensions' are organized around a cross-consistency matrix (marked as a cube for the 3D case on Fig.1).

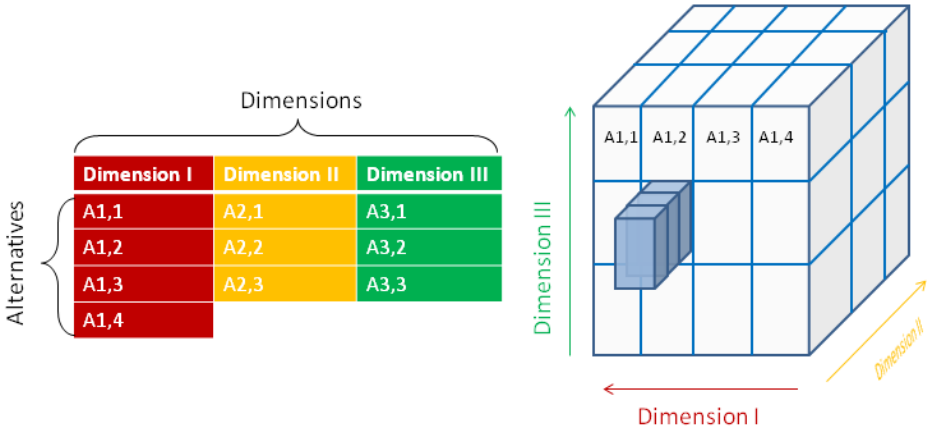

Fig.1. Graphical interpretation of the morphological analysis cross-consistency matrix.

Here it should be noted that the resulting scenario context practically encompasses one alternative from each dimension and the maximum number of possible scenarios is: $N_{max} = n \times m_1 \times m_2 \times \ldots \times m_i$, $i = 1, \ldots, n$. For the depicted in Fig.1 example $N_{max} = 3 \times 4 \times 3 \times 3 = 108$.

III. Software Implementation

The practical implementation of the morphological analysis requires expensive specialized software solutions (e.g. CASPER®, Think Tools® or J-DARTS®). In the present approach we are utilizing an own ad-hoc ones – I-SCIP-MA software [7]. The depicted in Fig.2 model encompasses data, gathered from discussions and q-based surveys, including 65 experts on national level and some supported information from an EU SySSec project survey, that relies on 75 international experts around new European Cybersecurity Red Book. Five key dimensions with different alternatives number are used: *Devices*: 'Mobile Smart Devices', 'Home Entertainment Systems', 'Home Automation Systems'; *Activities*: 'Entertainment', 'Communication', 'Everyday Work', 'Household Support'; *Communication Medium*: 'Cable Networks', 'Wireless Networks', 'Social Networks'; *Environment Characteristics*:

'Physical', 'Structural', 'Functional'; *Human Factor Characteristics*: 'Bioelectrics', 'Spacial', 'Sensual'.

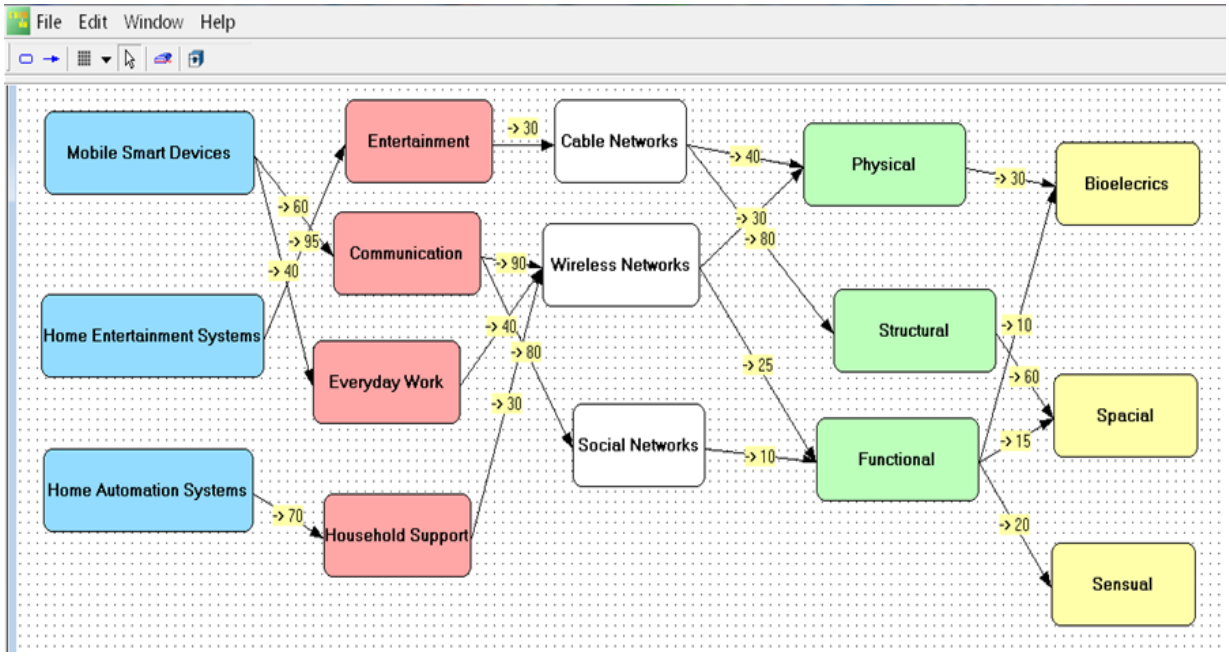

Fig.2. A screen shot from I-SCIP-MA environment model for smart homes cyber threats identification.

Here it should be noted that the key idea is to use objects (entities, marked as entitled, colorized round rectangles) which are connected with weighted relations (marked as labeled headed arrows), using the following percentages scale: weak [0-30]; moderate [30-50]; strong [50-100]. The sign of the weights determines their character: positive or negative. In the presented example only positive weights have been used for simplicity. As far as some of the entities, used in the model as dimensional alternatives are rather general, some details will be further given.

The *Devices* dimension covers: 'Mobile Smart Devices' alternative: smartphones, padfones, ultrabooks, tablets, smart watches and i-pods; 'Home Entertainment Systems' include: gamming consoles, robot companions, smart TVs, multimedia equipment, virtual/augmented reality devices; 'Home Automation Systems' covering security alarms, utilizing different sensor systems for areal, floor, movement, temperature, energy, etc. monitoring, smart household equipment devices control, automated lighting, doorkeeping and windowing;

The *Activities* and *Communication Medium* dimensions have been proposed from our experts' understanding keeping simplicity and paying attention to the current web technologies progress. The *Environment Characteristics* and *Human Factor Characteristics* have to be shortly explained. The 'Physical' environment characteristics cover a number of available parameters: atmosphere composition and pressure dynamics, t^{o}, light intensity, etc. (see e.g. the system described in [8]), whilst the 'Structural' and 'Functional' alternatives have to be considered in regards to parameters, like: internal design, functionality, suitability and ergonomity in respect with *Activities* and *Communication Medium* dimensions alternatives.

Finally, the *Human Factor Characteristics* dimension includes different 'Bioelectrics' (brain, heart, muscles activities, skin conductance, etc.), 'Special' (postural dynamics, space coordinates by means of

location, distance passed) and ‘Sensual’ (covering emotions, odor, tactile, sound, taste or visual human factor registered or self-reported reactions).

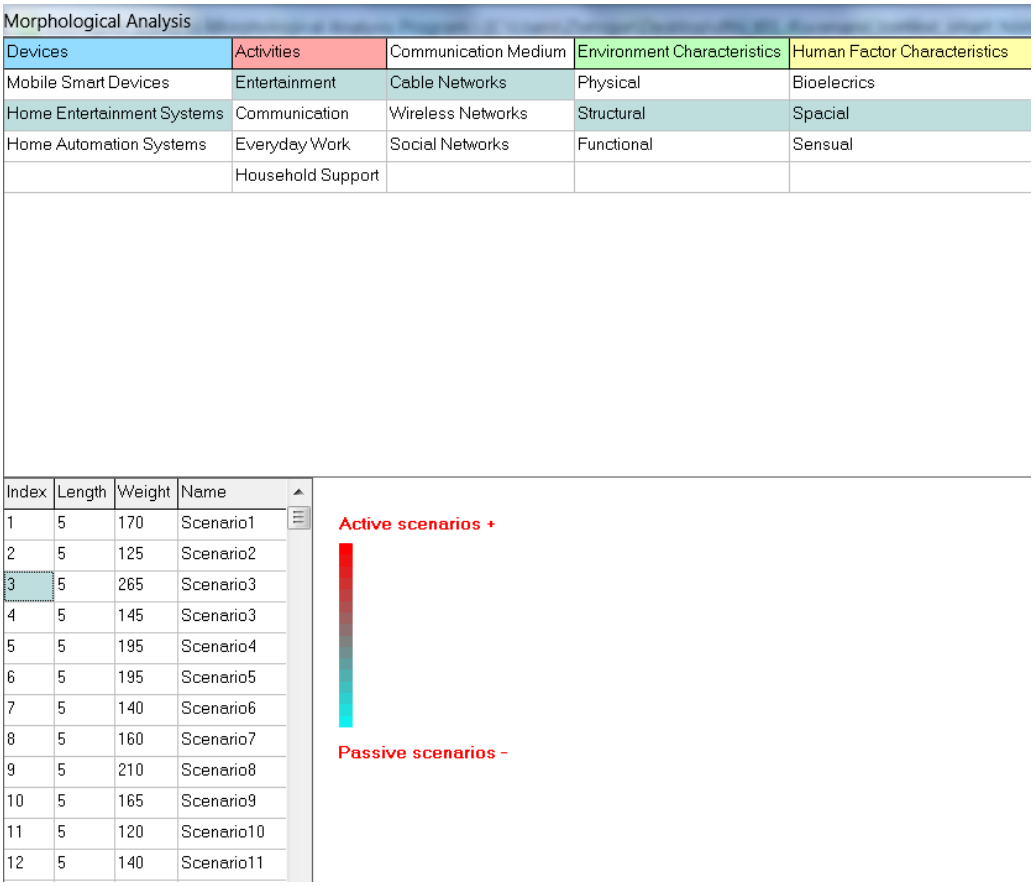

Fig.3. A screen shot of the generated scenarios set in I-SCIP-MA from the morphological model.

As it is clear from Fig.3 the different scenarios combinations have different Relative Common Weights (RCW) expressed as an additive percentage sum defined from the experts. In the present example a scenario set (plausible future) for identification of cyber physical threats, regarding smart homes is encompassing 21 scenarios and the most prominent of them (according to our experts ’knowledge) are: Scenario 3 (RCW = 265, including alternatives: ‘Home Entertainment Systems’ → ‘Entertainment’ → ‘Cable Networks’ → ‘Structural’ → ‘Spacial’), Scenario 9 (RCW = 210, including alternatives: ‘Mobile Smart Devices’ → ‘Communication’ → ‘Wireless Networks’ → ‘Physical’ → ‘Bioelectrics’) and Scenario19 (RCW = 110, including alternatives: ‘Mobile Smart Devices’ → ‘Everyday Work’ → ‘Wireless Networks’ → ‘Functional’ → ‘Bioelectrics’).

Discussion

The proposed framework for smart homes threats identification based on cyber-physical system modeling, combined with morphological analysis incorporates experts’ knowledge and high-level studies literature data. As far as the exploration of new technological trends requires both comprehensive and flexible approach, the proposed ones is found to be suitable enough for building a specific narrow context, based on scenarios. What however, is important to note here, is that this general solution does not give a complete answer to the detailed nature of cyberthreats origin but practically outlines first steps in the cyber-physical automated threats identification security systems.

A further more detailed study of the problem requires a system analysis, combined with experimental simulation, monitoring and validation of the experts' assumptions for real and reliable threats assessment based on agent-based paradigm. This will practically produce a preliminary classification of the smart homes cyber-physical systems entities that are re-classified with the help of sensor information embedded in virtual agents and used for improving the future smart homes and cities inhabitants' security.

Acknowledgement

This publication is financially supported by DFNI-T01/4 'A Feasibility Study on Cyber Threats Identification and their Relationship with Users' Behavioural Dynamics in Future Smart Homes', National Science Fund, Ministry of Education, Youth and Science, 2012 – 2014, www.smarthomesbg.com. The authors also express a special gratitude for the experts' data support to EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet – SySSec FP7 project, Grant Agreement No 257007, 2007 – 2013, www.syssec-project.eu.

References

[1]. Chourabi, H. et al, Understanding Smart Cities: An Integrative Framework, System Science (HICSS), 45th Hawaii International Conference on System Sciences, 2012, 2289-2297.

[2]. De Silva, L.C., Mirokawa, Ch., Petra M. I., State of the Art of Smart Homes, Engineering Applications of Artificial Intelligence, 2012, Available at: http://dx.doi.org/10.1016/j.engappai.2012.05.002

[3]. Internet Security Threat Report, Symantec, Volume 18, April, 2013, Available at: http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf

[4]. Mary Meeker & Liang Wu, Internet Trends Report, D11 Conference, Rancho Palos Verdes, California, May 28-30, 2013, Available at: http://allthingsd.com/20130529/mary-meekers-internet-trends-report-is-back-at-d11-slides/

[5]. Security Threats Report 2013, Sophos, Available at: http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf

[6]. Strategic R&D Opportunities for 21st century Cyber-Physical Systems, Report of th Steering Commitee for Foundations and Innovations in Cyber-physical Systems, January, 2013, Available at: http://www.nist.gov/el/upload/12-Cyber-Physical-Systems020113_final.pdf

[7]. Zlatogor Minchev & Velizar Shalamanov, Scenario Generation and Assessment Framework Solution in Support of the Comprehensive Approach, In Proceedings of SAS-081 Symposium on "Analytical Support to Defence Transformation", RTO-MP-SAS-081, Sofia, Boyana, April 26 – 28, 22-1 – 22-16, 2010.

[8]. Георгиев С. Колев Х. Обрешков Н. Лалев Е. Система за сигурност в домовете на бъдещето. „Сборник материали - HOME/2010/CIPS/AG/019", Част втора, ISBN 978-954-92552-7-0, 2013.