Smart Homes Cyberthreats Identification Based on Interactive Training

Zlatogor Minchev[1], Luben Boyanov[2]

Institute of Information and Communication Technologies, Bulgarian Academy of Sciences

Acad. Georgi Bonchev Str., Bl. 25A, zlatogor@bas.bg[1], lb@acad.bg[2]

Abstract. The paper briefly describes cyber threats identification framework in a smart home test bed environment. A problem space is initially built, through a q-based survey of potential cyber threats sources. Further on, an expert based reference with morphological and system modelling and analysis of this space is performed via a specialized software environment – I-SCIP-MA-SA. The validation is organized through an interactive human-machine agent based constructive simulation. Selected users' and environment characteristics are monitored for the proposed identified threats validation. This assures an explanatory cyber threats identification combined with real test bed experiments through interactive training.

Key words. cyber threats, smart homes, morphological and system analysis, agent based simulation, constructive simulation, interactive training.

1. Introduction

Today smart homes are becoming an indispensible modern part of our everyday live. This concept has gone through a significant evolution for almost a century and nowadays is addressing telemedicine, security and emergency areas, green energy and emerging technologies. This is also a result of the current fast ICT progress and opens a number of threats for the technologies development perspectives and their users' response.

The modern IT world is a place where the interactiveness between technologies and humans' is constantly evolving, mixing physical and digital realities. Humans are becoming more and more significant, with special attention paid to the behaviour dynamics and ambient factors influence. This could be a useful information source in the analysis of cyber threats for smart homes.

The paper briefly considers a methodological framework for identifying cyber threats on the basis of experts' believes, filtered with morphological and system analysis. The results are further experimentally validated in a test bed environment for a selected scenario sets. The process is organized around a multi-agent constructive simulation concept with human-in-the-loop participation. During this, the activities of the test bed inhabitants (smart homes users) and environment conditions are monitored for experimental correlation of selected scenarios sets.

This useful combination is producing a promising base for empirical validation of experts' believes through interactive training and constructive simulation. Further on, the paper gives a more detailed description of the proposed idea.

2. Methodological Framework

Generally, the methodological framework for cyber threats identification (see Figure 1) encompasses the application of the "scenario method" combined with analysis and validation. Both implementing experts' believes and real human-in-the-loop monitored participation through agent based constructive simulation.

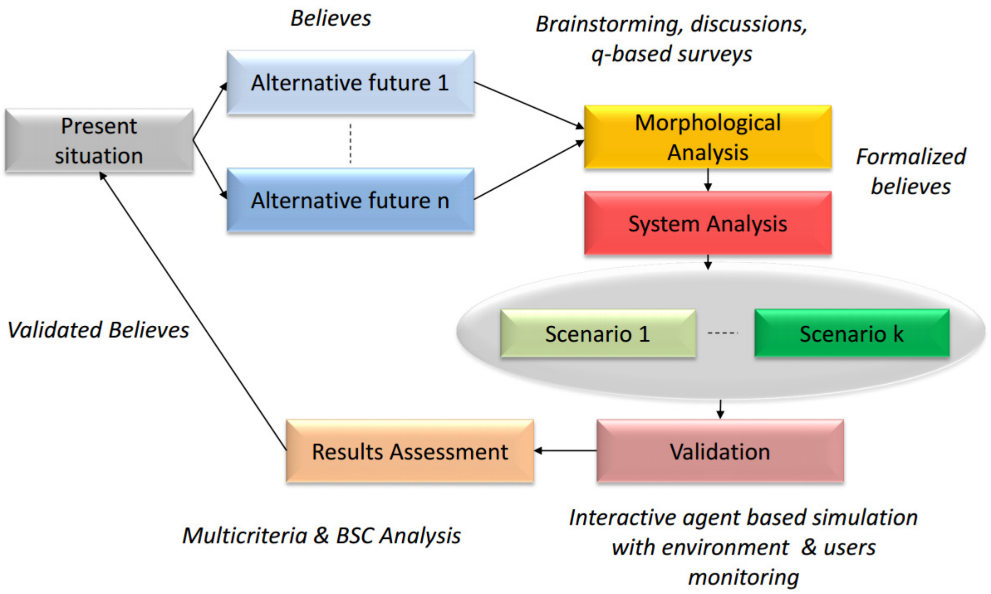


Figure 1. General schematic representation of the methodological framework.

The methodological framework, presented on Figure 1 could be practically implemented for smart homes cyber threats identification in four stages: (i) cyber threats identification, (ii) context definition, (iii) analysis and (iv) validation [11]. The next section gives more details of this four stages practical implementation.

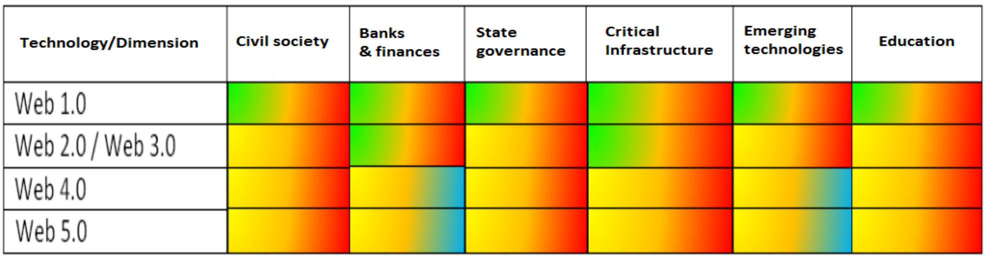
3. Practical Implementation

Cyber threats identification was performed collecting users' focus group data gathered from two q-based surveys.

The first survey concerned Web technologies trends for a five years' time horizon and expected cyber threats in several social facets (*Civil Society*, *Banks and Finances*, *State Governance*, *Critical Infrastructure*, *Emerging Technologies*, *Education*). A focus group of 150 participants (national and international experts) has been studied [11].

The second survey results were produced from 250 participants' focus group at the University of National & World Economy – Sofia, The College of Telecommunications and Post and VISENSI Ltd. The obtained trends were covering: "*Type of used smart devices"*; "*Activities for using smart devices*"; "*Positives of using smart devices with Internet access"*; "*Negatives of using smart devices with Internet access"*; "*Type of information exchanged via smart devices*"; "*Smart devices influence to everyday life*".

A generalization of the obtained results from both surveys is presented in Figure 2 and Figure 3.



Technology/Dimension	Civil society	Banks & finances	State governance	Critical Infrastructure	Emerging technologies	Education
Web 1.0						
Web 2.0 / Web 3.0						
Web 4.0						
Web 5.0						

Figure 2. Q-based survey results about Web technologies trends amongst 150 participants.

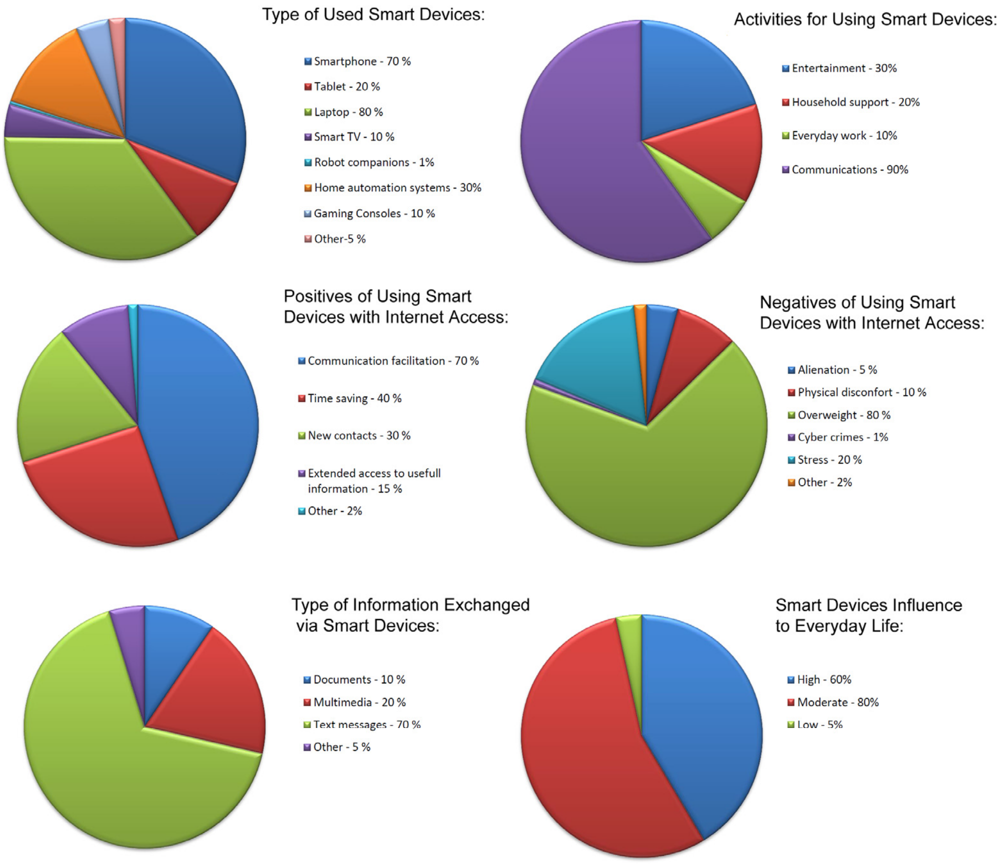


Figure 3. Q-based survey generalized results of smart devices amongst 250 participants.

The notations from Figure 2 [11] are using a discrete five-level color scale from "green" to "red" trough "yellow" that shows an increasing influence towards red and a decreasing one – towards green. The "blue" color is noting uncertainty. Similarly to another recent EU study, the selected time horizon was five years [1].

Briefly, the resulting trends are marking cyber risks and threats' importance increase in all Web 1.0/Web 5.0 technological areas. A visible exception of the part concerning Web

4.0/Web 5.0 (for *Banks and Finances* and *Emerging Technologies* facets) is quite understandable as these new technologies are expected to be available in at least ten-year time horizon.

The generalized results from Figure 3 demonstrate that most of studied the users are relying on *Smartphones* (70%) and *Laptops* (80%) for *Communication* (90%) and *Entertainment* (30%). A few of them are using smart devices for *House hold support* (30%), including: automated washing machines, drying machines, cleaning and cooking robots, dishwashers. Only 10 % from the users are having *Smart TVs* and *Gamming consoles*.

According to the studied users' focus group, the positives of smart devices usage are related to: *Communication facilitation* (70%) and *Time saving* (40%). The creation of *New contacts* is 30% of the users' priorities. The negatives are given to *Overweight* (80%) and *Stress* (20%). Mobile smart devices are most often used for text messages exchange (70%) and multimedia (20%). Currently the influence of smart devices influence to our everyday lives is classified as *Moderate* (80%) up to *High* (60%). The percentages sum is over a hundred, as the participants were allowed to give more than one answer.

Context definition is the second stage following cyber threats identification. Graphically, it is summarized in Figure 4:

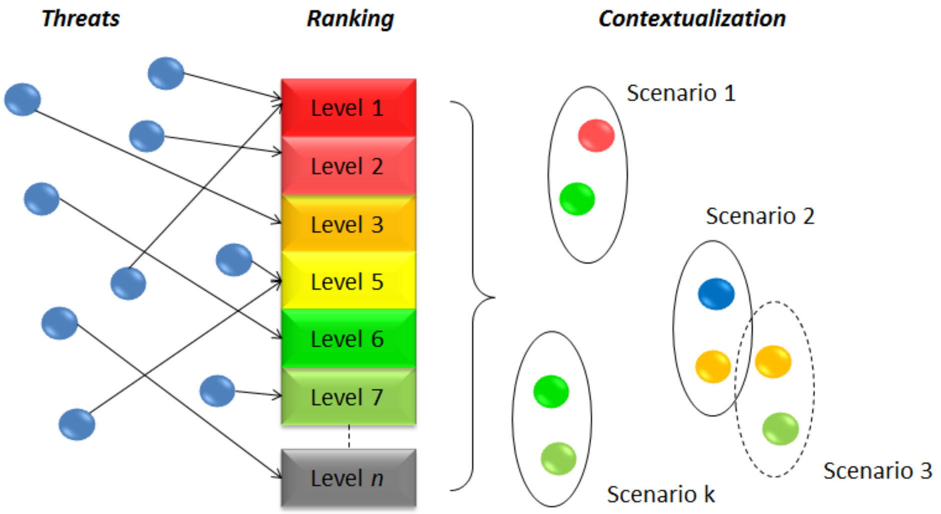


Figure 4. Graphical interpretation of the context definition process.

The identified cyber threats are arranged in accordance with their importance using experts' opinion. The results are implemented as driving factors [13] for the morphological and system analysis during scenarios preparation (see next stage). A good comprehensive example is the recent SysSec consortium study [7]. The authors mark three basic directions: "mobile devices", "social networks", "critical infrastructure".

A classification regarding smart homes environment, presented in Table 1 was proposed by the authors [2].

SMART HOME SERVICES	POSSIBLE THREATS	CRITICAL ATTACK POINTS	POSSIBLE CONSEQUENCES FROM THE ATTACK
Health care	Do not take medicine, pacemaker malfunctioning, etc.	Sensors, video surveillance, communication system, integrating system, external communications	Critical
Care for children or people with disabilities	Requires attention	Sensors, video surveillance, communication system, integrating system, external communications	Critical
Security and safety	Intrusion	Sensors, video surveillance, communication system, integrating system, external communications	Critical
Care for children or people with disabilities	Requires attention	Sensors, video surveillance, communication system, integrating system, external communications	Critical
Home environment	Fire, flooding, gas leakage	Sensors, video surveillance, communication system, integrating system, external communications	Critical
Smart home appliance	Does not turn off, turns on/off at wrong time	Sensors, video surveillance, communication system, integrating system	Non-critical, but dangerous
Privacy	Violation of privacy, data gathering	Video surveillance, communication system, integrating system, external communications	Non-critical but dangerous
Entertainment and pleasure	Malfunctioning of the pleasure, comfort and entertainment systems	Sensors, communication system, integrating system	Non-critical

Table 1. Services, dangers, attack points and consequences in smart homes.

The results from Table1 are practically used during the analysis and validation methodological stage.

The **Analysis** is performed in four sub stages. As far as the scenario method has been selected for methodological base, morphological and system analyses are initially performed.

Generally, these processes are relying on experts' data with a lot of combinations and uncertainties, so some software support with I-SCIP-MA-SA [8] is also implemented.

The key idea for machine interpretation of the problem space is the E-R paradigm [3] graphically represented with named round rectangles (Entities) and weighted headed arrows (Relations).

Morphological analysis

A resulting problem space for smart homes cyber threats scenarios exploration through morphological analysis with 16 alternatives spread in 5 dimensions [9] is shown on Figure 5. The dimensions are presented in different colors.

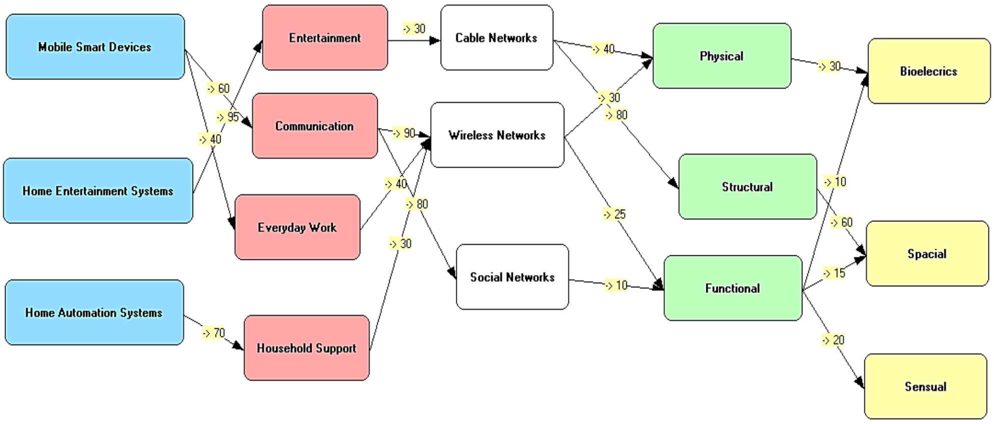


Figure 5. A screen shot of I-SCIP-MA for morphological scenario problem space with 16 alternatives and 5 dimensions, studying smart homes cyber threats.

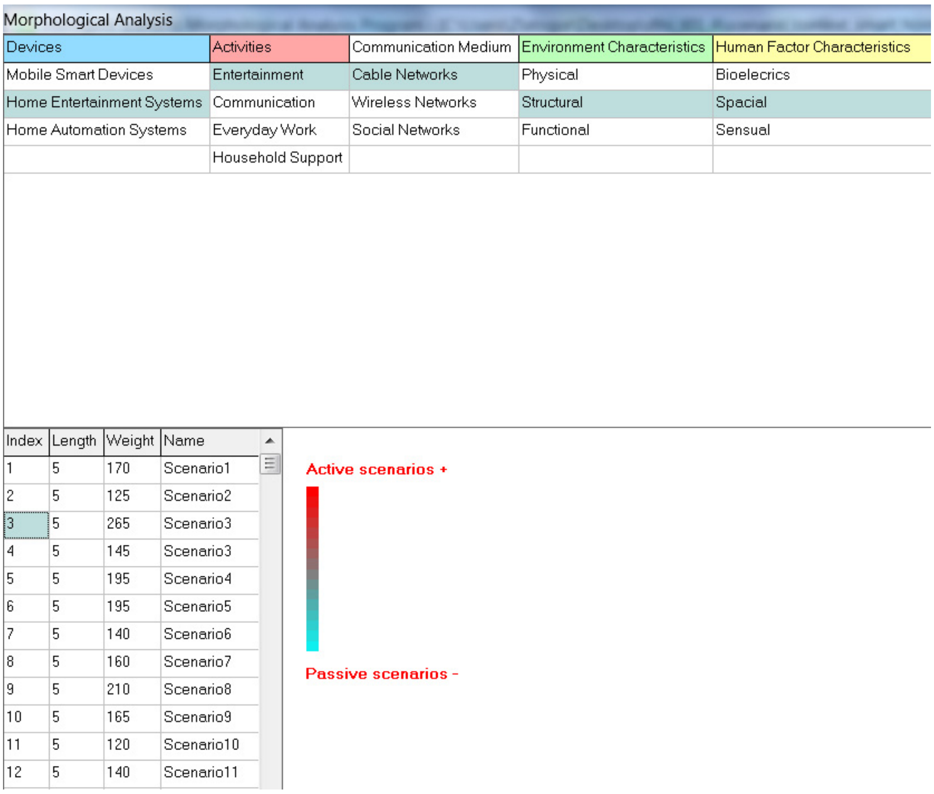
The resulting cross-consistency matrix contains *N* = 1620 (*N* = 5 x 3 x 4 x 3 x 3 x 3) scenario combinations (see Figure 6). It is important to note here, that the implemented scale for weighting the arrows gives the percentage measure, covering three levels: weak [0-30%], moderate [30-50%], high [50-10%] from the interval [0, 1].

The *Dimensions* part is encompassing the following: "Devices", "Activities", "Communication Medium", "Environment Characteristics", "Human Factor Characteristics". Each dimension contains different number of alternatives that in practice are subspaces, e.g. "Devices" encompasses: "Mobile Smart Devices", "Home Entertainment Systems" and "Home Automation Systems".

A ranking, using Relative Common Weight (RCW) has been performed. RCW sums the unidirectional relations' weights (noted with yellow labels above the relations) connecting an alternative from each of the five dimensions that were used. The final results are scenarios with negative or positive RCW in accordance with obvious or hidden cyber threats identification.

The most interesting scenario combinations in our morphological analysis were: Scenario 3 (RCW = 265, encompassing: "Home Entertainment Systems" → "Entertainment" → "Cable Networks" → "Structural" environment characteristics → "Spacial" human factor characteristics); Scenario 9 (RCW = 210, encompassing: "Mobile Smart Devices" → "Communication" → "Wireless Networks" → "Physical" environment characteristics → "Bioelectric" human factor characteristics) and Scenario 19 (RCW = 110, encompassing:

"Mobile Smart Devices" → "Everyday Work" → "Wireless Networks" → "Functional" environment characteristics → "Bioelectric" human factor characteristics).



Morphological Analysis

Devices	Activities	Communication Medium	Environment Characteristics	Human Factor Characteristics
Mobile Smart Devices	Entertainment	Cable Networks	Physical	Bioelecrics
Home Entertainment Systems	Communication	Wireless Networks	Structural	Spacial
Home Automation Systems	Everyday Work	Social Networks	Functional	Sensual
	Household Support			

Index	Length	Weight	Name
1	5	170	Scenario1
2	5	125	Scenario2
3	5	265	Scenario3
4	5	145	Scenario3
5	5	195	Scenario4
6	5	195	Scenario5
7	5	140	Scenario6
8	5	160	Scenario7
9	5	210	Scenario8
10	5	165	Scenario9
11	5	120	Scenario10
12	5	140	Scenario11

Figure 6. A screen shot from I-SCIP-MA of morphological cross-consistency matrix with $N = 1620$ scenario combinations for smart homes cyber threats exploration.

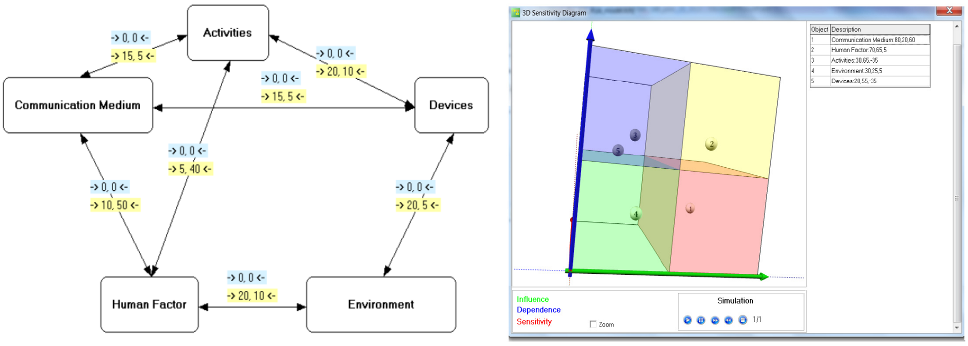
These results do not give any concrete cyber threats identification scenarios but just outline, in accordance with the experts believes, the importance of the activities "Entertainment", "Communication" and "Everyday Work" together with the human factor "Spacial" and "Bioelectric" characteristics in smart home environment.

System Analysis

Generally, the system analysis for a smart home is a complex dynamic system approximation. The system model for smart homes could be both static [2] and dynamic. Whilst, the static one gives general classification of the objects of interest, the dynamic is quite useful in the *Validation* process. It is important to note that the E-R paradigm is used implementing weights (with similar to the morphological analysis scale) and time of the bidirectional relations (both noted, consecutively with labels in yellow and blue).

Additionally, a three dimensional Sensitivity Diagram (SD) presenting influence (x), dependence, (y) and sensitivity (z). Four sectors encompassing the entities classification are utilized: green (buffering), red (active), blue (passive) and yellow (critical). All entities from the model are visualized in SD with indexed balls.

Practical illustration of a static smart home general system model and a resulting SD classification are given in Figure 7.



Object	Description
1	Communication Medium:80,20,60
2	Human Factor:70,65,5
3	Activities:30,65,-35
4	Environment:30,25,5
5	Devices:20,55,-35

Figure 7. A smart home system model (left) and resulting SD diagram (right) after [2].

The resulting SD from Figure 7 gives a profitable classification for further analysis, outlining the "Human Factor" (indexed ball/sphere "2" with coordinates {x=70, y=65, z=5}) as a critical entity together with the potential hidden cyber threats passive entities: 'Devices'(indexed ball "5" with coordinates {x=20, y=55, z = -35}), "Activities" (indexed ball "3" with coordinates {x=30, y=65, z= -35}) and real active one: "Communication Medium" (indexed ball "1" with coordinates {x=80, y=20, z=60}).

Further *Validation* was performed trying to obtain more comprehensive evidence for this experts' believes and analyses results.

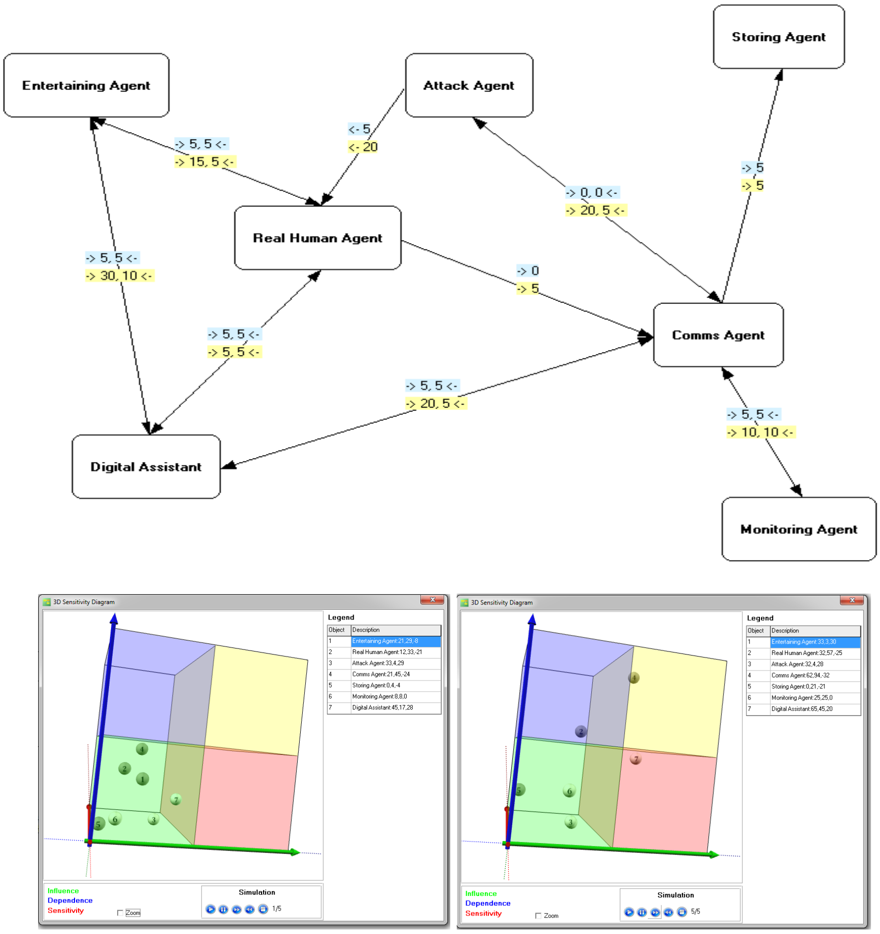
Validation

This final stage of the presented methodological framework is related to interactive training and includes agent-based modeling and simulation. The presented multi-agent model, implemented in I-SCIP-SA dynamic environment (see Figure 8) is encompassing seven key role agents: "Real Human Agent", "Entertaining Agent", "Comms Agent", "Storing Agent", "Monitoring Agent", "Digital Assistant", "Attack Agent". Generally these roles cover a number of devices, protocols and parameters. What is important to note here is the capability for connecting real devices with simulated ones, i.e. mixing the virtual and real world. Additionally, Figure 8 illustrates the initial believs evolution, starting from green and progressing towards different SD sectors in accordance with model relations weights' dynamics.

As the human factor in this dynamic model (noted with indexed "2" sphere) is classified as a passive one (blue sector of SD on Figure 8) a more detailed analisys could be performed trough a test bed interactive environment.

For this purpose, a smart home test bed environment (see Figure 9) has been organized in the framework of DFNI T01/4 project at the Institute of Information and Communication Technologies (IICT), Bulgarian Academy of Sciences – BAS.

The test bed environment is positioned in a room equipped with a number of smart devices, including: 3D TV/monitors, X-box game console, entertainment and cleaning robots, programmed tablet remote control and IP video omnidirectional monitoring system. An ad-hoc created digital assistant - "Alex", provides voice control for lighting, multimedia and heating with holo-like projection avatar. In addition, an environment embedded Xbee sensor barometer system and wearable human factor bio headband are being developed [4]. The sensor barometer system is also capable to monitor CO/CO2 concentration measurement, radiation, electromagnetic fields and dust particles [5].



Legend

Object	Description
1	Entertaining Agent:21,29,-8
2	Real Human Agent:12,33,-21
3	Attack Agent:33,4,29
4	Comms Agent:21,45,-24
5	Storing Agent:0,4,-4
6	Monitoring Agent:8,8,0
7	Digital Assistant:45,17,28

Legend

Object	Description
1	Entertaining Agent:33,3,30
2	Real Human Agent:32,57,-25
3	Attack Agent:32,4,28
4	Comms Agent:62,94,-32
5	Storing Agent:0,21,-21
6	Monitoring Agent:25,25,0
7	Digital Assistant:65,45,20

Figure 8. Basic multi-agent system model representation with 5 steps dynamics.

The human factor activities are monitored via EEG Nation 7128W – C20, bio headband for ECG and body temperature monitoring [4]. All data from sensors and video behavior monitoring is stored in a data base.

Figure 9. Moments of smart home test bed validation usage at IICT-BAS.

The above described test bed has been organized for practical agent-based interactive training.

Some interesting results have been recently published [12] concerning the human factor hidden threats related to EEG dynamics in 2D and 3D visual environment and the gamming process in social networks. The results directly accentuate the necessity of comprehensive study of cyber threats problem in smart homes and the emerging “digital drugs” [6]. We are planning further improvement of the validation process with other users’ behavioural modalities. The results will be evaluated via multicriteria analysis and balanced score card [10].

Discussion

The progress in smart homes technologies is opening a number of cyber threats to their users today. Whilst some of them are quite obvious, other related to entertainment, privacy and appliances are hiding a lot of unexplored domains. Examples for such new cyber threat areas are the digital drugs (addiction to technologies) and social engineering that are important for the future generations of inhabitants (users) of smart homes.

A suitable framework approach for studying these problems is the combination of experts’ believes data, analysis, modelling, inhabitants and environment monitoring, as well as, practical validation through real constructive experimental training.

Acknowledgement

The results in this publication are financially supported by: “A Feasibility Study on Cyber Threats Identification and their Relationship with Users’ Behavioural Dynamics in Future Smart Homes”, Research Grant “Funding of Fundamental & Applied Scientific Research in Priority Fields”, Bulgarian Science Fund, Ministry of Education Youth and Science, 2012-2014, DFNI-T01/4, www.smarthomesbg.com. A special gratitude for the threats identification methodology is also given to: “EU Network of Excellence in Managing Threats and Vulnerabilities for the Future Internet” – SysSec, FP7 Grant Agreement No. 257007, 2010 – 2014, www.syssec-project.eu

References

1. Balzarotti, D. Second Report on Threats on the Future Internet and Research Roadmap, SysSec Consortium Deliverable D4.2, September, 2012, http://www.syssec-project.eu/m/page-media/3/syssec-d4.2-future-threats-roadmap-2012.pdf [Online]

2. Boyanov, L., Minchev, Z. Cyber security Challenges in Smart Homes, In Proceedings of NATO ARW “Best Practices and Innovative Approaches to Develop Cyber Security and Resiliency Policy Framework”, Ohrid, Macedonia, June 10-12, 2013 (in press)

3. Chen, P. The Entity-Relationship Model-Toward a Unified View of Data, ACM Transactions on Database Systems, 1, no.1, 9–36, 1976.

4. Georgiev, S., Minchev, Z. An Evolutionary Prototyping for Smart Home Inhabitants Wearable Biomonitoring’, In Proceedings of Conjoint Scientific Seminar “Modelling & Control of Information Processes”, IMI-BAS, 21 – 31,`November 19, 2013.

5. Georgiev, S., Kolev, H., Obreshkov, N., Lalev, E. Security System for Future Smart Homes, In Proceedings of National conference with international participation in realization of the EU project “Development of Tools Needed to Coordinate Inter-sectorial Power and Transport CIP Activities at a Situation of Multilateral Terrorist Threat. Increase of the Capacity of Key CIP Objects in Bulgaria”, at Grand Hotel “Sofia”, Sofia city, Bulgaria, June 4, 91-100, 2013 (in Bulgarian).

6. Guma, G. Messing with Our Minds: Psychiatric Drugs, Cyberspace and “Digital Indoctrination”, Global Research, November 11, 2013, http://www.globalresearch.ca/messing-with-our-minds-psychiatric-drugs-cyberspace-and-digital-indoctrination/5357710 [Online]

7. Markatos, E., and Balzarotti, D. (Eds) The Red Book. The SysSec Roadmap for Systems Security Research, The SysSec Consortium, 2013, http://www.red-book.eu/m/documents/syssec_red_book.pdf [Online]

8. Minchev, Z., Shalamanov, V., 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, http://www.gcmarshall.bg/KP/new/MP-SAS-081-22-MINCHEV-SHALAMANOV.pdf [Online]

9. Minchev, Z., Boyanov, L., & Georgiev, S. Security of Future Smart Homes. Cyber-Physical Threats Identification Perspectives, In Proceedings of National conference with international participation in realization of the EU project 'Development of Tools Needed to Coordinate Inter-sectorial Power and Transport CIP Activities at a Situation of Multilateral Terrorist Threat. Increase of the Capacity of Key CIP Objects in Bulgaria', Grand Hotel 'Sofia', Sofia, Bulgaria, 165-169, June 4, 2013.

10. Minchev et al., Joint Training Simulation and Analysis Center, Technical Report, Institute for Parallel Processing, Bulgarian Academy of Sciences, 2009, http://www.gcmarshall.bg/KP/new/jtsac_tr.pdf [Online].

11. Minchev, Z. Security of Digital Society. Technological Perspectives and Challenges, In Proceedings of Jubilee International Scientific Conference “Ten Years Security Education in New Bulgarian University: Position and Perspectives for the Education in a Dynamic and Hardly Predicted Environment” Sofia, Planeta -3 Publishing House, 438-444, 2013 (in Bulgarian)

12. Minchev, Z. 2D vs 3D Visualization & Social Networks Entertainment Games. A Human Factor Response Case Study, In Proceedings of 12th International Conference, ICEC 2013, São Paulo, Brazil, October 16-18, 2013 (Editors: Junia C. Anacleto, Esteban W. G. Clua, Flavio S. Correa da Silva, Sidney Fels, Hyun S. Yang), Lecture Notes in Computer Science, vol. 8215, 107-113, 2013b.

13. Schwartz, P. The Art of the Long View: Planning for the Future in an Uncertain World, Doubleday Currency, New York, 1991.