CYBER SECURITY CHALLENGES IN SMART HOMES

Luben Boyanov & Zlatogor Minchev

Institute for Information and Communication Technologies – Bulgarian Academy of Sciences

SMART HOMES HISTORICAL ORIGINS

Smart homes have emerged because people wanted to improve and optimize the comfort in their homes, minimizing at the same time daily home responsibilities. The first automated home systems have been presented at the Chicago and New York World Fairs in 1934 and 1939. Introducing more wires in the home was carried out by some hobbyists in the 1960-ies but at the time, technologies did not offer too many options for optimization and efficiency in the house. The expression "smart house" is regarded first to be used by the American Association of Housebuilders in 1984 [1].

Despite the growth and advances in electronics – namely the appearance of microcontrollers, microprocessors, RAM and ROM memory, and also the emergence of smaller and less expensive household appliance, smart homes have been built only by the very rich and geeks until the late 1990-ies. At the same time, home security systems intrusion and fire detection became widespread for most households. Since the start of the 21-st century, with the penetration of personal computers, Internet, cell phones, and wireless networks in every home, the situation started changing. A significant reason for the change of trend was also the emergence of cheap, autonomous wireless sensors, passive and active identification tags – RFID. The home became a ground for introducing and implementing technological advances.

SMART HOMES TODAY

Nowadays, the term "smart home" is used for a house with technological equipment for control, monitoring, automation and optimization of:

- Home environment – temperature, humidity, air purity, house light, etc.
- Home security and safety – burglary, fire, smoke, carbon monoxide, gas, etc.
- Inhabitants and their health – children, elderly people, disabled, etc.
- Household appliances – air conditioning, gas or electric cooker, refrigerator, TV, video and audio systems, etc.
- Energy efficiency – electricity, gas, water, etc.

Examples of smart homes are most common in countries with advanced economies like the USA [2], [3], [4], Japan [5], [6], [7] and EU [8], [9], [10]. In addition to the advances in various technologies mentioned above, another factor influencing the wider implementation of smart homes is that energy use in residential and commercial buildings, in developed countries is between 20 and 40% [11]. Towards such implementation will contribute the estimate that average household energy consumption can reduce its carbon emissions by 71% and annual energy cost – by 105% [12]. Some 1.5 million automation systems have been installed in the USA in 2012, doubling the shipments from the previous year, with an estimate this number to raise to 8 million per year in 2017 [13].

SMART HOMES FEATURES

As mentioned above, the term "smart home" is used for dwellings equipped with technologies that allow monitoring of its environment and inhabitants. The equipment can actively react to the occurrence of an event. A simple example of active reaction is when somebody enters the house and does not enter the correct security alarm code or when there is fire or smoke and it is detected by the monitoring system and an alarm is set or the owner is informed by a prerecorded message sent over the phone (cell or landline). Another example for "simple" behavior of smart devices is when somebody enters a room and the light goes on. Such situations and use of automation at home are rather popular but they do not require much of intelligent data processing. However, if we look at a situation when one must find out if an elderly person or a child is home alone, or whether they feel comfortable and need no attention, or if some of them had fallen on the floor and do not feel well, so there is a potential danger – the task for taking an appropriate action during such scenario is much harder.

This is how we move to a higher level of "smart" processing of data – those indication trouble or problems are to be detected by sensor or multimedia sources in the smart home, possibly saved, and then treated by an intelligent system (a computerized one). The last action is likely to include some assessment in regard to data or a scenario, given in advance, and on the basis of thresholds specified in the system. It is also possible that in terms of energy efficiency optimization, monitoring and control of devices and appliances can be carried out in the house. Such activities can be realized today due to the advances in electronics – sensor devices, video and audio surveillance, computers, and various types of networks that connect all modules in the house.

Different examples on the state and varieties of a smart home are presented in [14] and [15]. Summarizing the applications, a smart home contains:

- Various sensors in rooms and other house areas with some activity– including on the floor, where they can detect whether a person or an object has fallen
- Systems for monitoring health function of the inhabitants of the home
- Sensors and systems for home safety monitoring
- Systems for monitoring pets, appliances or the state of an object
- Devices that control lighting and temperature
- Systems that monitor and control entertainment, or outdoor (e.g. garden) equipment

This can be categorized as the lowest, ***first level*** – the ***detection*** level. All those sensors, systems and devices actively react to certain events, which ends an input to the ***second level*** that can be either an inhabitant of the house or a control and monitoring system – the ***perception*** level. The second level may or may not actively react to events from the first level. In case the house has a specialized control and monitoring system, it is usually connected to the sensors and detecting devices via some communication network. The connections may go also to an integrating intelligent center in cases when no direct reaction is expected – a simple example - security system records the area of intrusion, sets up a siren and dials a phone number to transmit a warning. This can be viewed as ***third level*** – ***intelligent integration*** level. It is possible that a reaction from outside to certain events in the house might be needed – so there must be a communication from the intelligent integrating center to the outside world. This can be regarded as the last, ***fourth level*** – ***outdoor*** level. External communication can be via cell-phone services or Internet and can aim at passing data to home owners or inhabitants, social and medical staff, or security services. Smart home architecture is depicted in Figure 1:

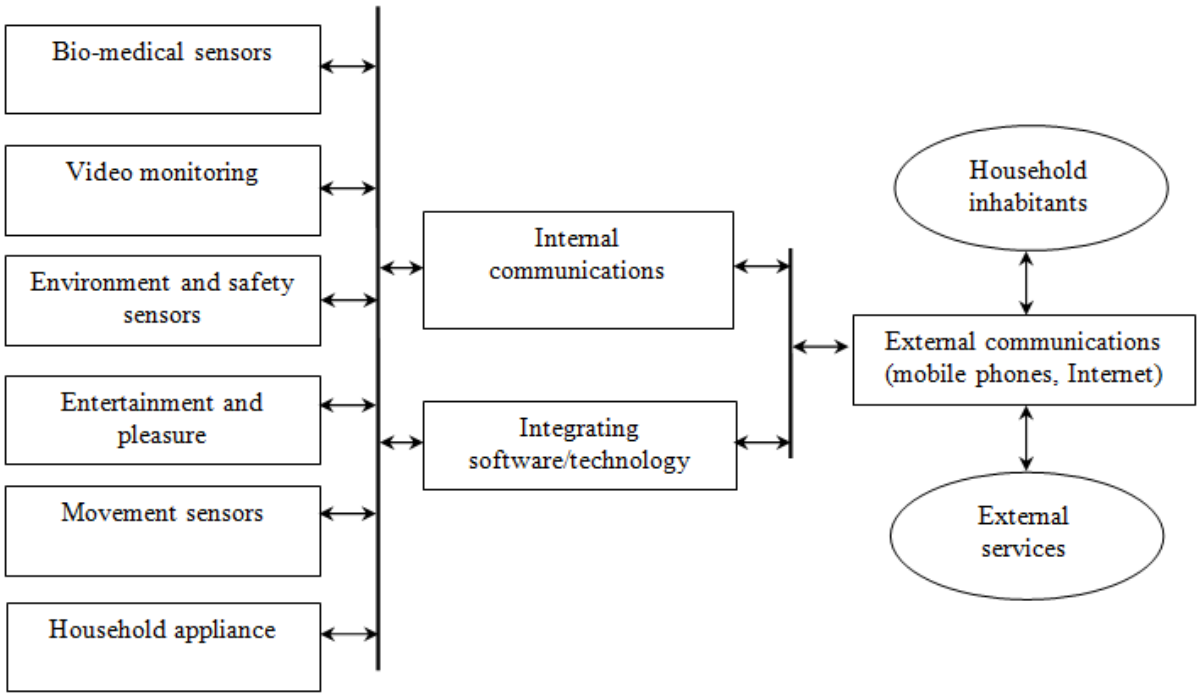

Figure 1. Smart home architecture.

The most important features that differentiate smart homes from other linked and controlled systems like global Internet, Municipal Area Networks (MAN) and office networks are:

- Lack of professional network or system administrator,
- The big heterogeneity of connected equipment – sensors, appliance, machines,
- The very high requirements for privacy, robustness, availability of services and denial of unauthorized access.

Smart home users in addition to very rich and/or geeky (the "rich geek toys" stereotype) are:

- People who live on their own and may be not capable of handling emergency situations by themselves,
- People with physical or medical problems – diabetics, cancer, asthma, Alzheimer, dementia, etc.,
- People living in remote or isolated areas, or places with no proper health care,
- Children.

Technologies

Sensor technology is the most important one used in smart homes. The recent advances in this field, including the emergence of low-cost and low-weight electronic circuits, novel manufacturing technologies and signal processing methods, allow their effective and efficient intrusion in the domain of smart homes [16]. Sensors work on optical, acoustic, thermoresistive, piezoresistive, capacitive, electromagnetic, piezoelectric principles. In the field of medicine, the micro-electromechanical

systems (MEMS) can detect triglycerides, c-reactive protein, and glucose, measure tissue softness during surgical procedures; count blood cells; measure intramuscular pressure, etc. [17]. Such advances allow data, gathered from sensors not only to monitor the home environment but also the activities and health status of smart home inhabitants.

In addition to the use of sensor technologies, home monitoring, can also be implemented using video surveillance and RFID technology. High-quality digital video IP camera with Internet network connectivity can provide the required clear video and images in both daylight and night, to be used by humans or processed by computer system. Major obstacles until a decade ago were the price of memory and the lack of proper technology for fetching critical information from the bulk of collected data, as such was only available for expensive, high-end computer systems. However, the present situation has changed and will continue doing so with the advent of time. Another, so far unresolved issue that hinders the benefits of video surveillance is privacy protection.

Another important technology is the RFID - Radio Frequency Identification, which is wireless non-contact use technology that uses radio-frequency to transfer data to and from tags attached to objects. Since 2004, many hospitals in the USA implant RFID tags to identify and track patients [18] and this technology is used for healthcare in smart homes [19]. RFID tags can be implanted within pets and even people. The fact that the implant carries personal identification, contact information and medical history, raises some security and privacy concerns [20].

Products, communication and integration

The most common products in regard to comfort, control and security are remote control devices, intrusion detection and home monitoring systems (security alarms, motion sensors, security cameras), and more recently – sensors and devices for biometric monitoring that can be attached or implanted in people, who require automated health care. Very popular are also mobile or stationary products and systems for control of physical (lighting, heating, cooling, noise) or chemical (gas, smoke) features and components.

The most common communication products at home at present are wired (Ethernet) and wireless (Wi-Fi) networks, devices and systems linked via infrared transceivers and Bluetooth. Other promising communication protocols are Z-Wave, ZigBee and HomePlug. ZigBee is an open wireless IEEE standard, which can be used in direct communications but is most often applied on a star or tree topology mesh network. It operates in the 2.4-GHz band with maximum data rate of 250 kbits/s. It has a typical power of 1 mW and free space range to about 10 meters. Z-Wave is a proprietary wireless standard with wireless mesh networking technology. It operates at 908.42 MHz in North America but uses other frequencies in other countries depending on the regulations. Data rates are 9.6 kbits/s and 40 kbits/s. Output power is 1 mW covering a range of up to 30 meter. Z-Wave and ZigBee are low power, short range wireless protocols that carry small messages to/from sensors and are likely to become the dominant communication technologies for Home Area Networks (HANs).

Integration systems consist of computers or similar intelligent systems that can “read” data, issued by sensors and monitoring devices. On the basis of the received data, these systems must be able to take decisions. So far there is no widespread integrating software for such system but a promising approach is being taken by Microsoft since 2010 with its HomeOS. Its version has been used in 12 real houses for periods of 4-8 months [21]. The operating system is designed to control the lighting, video surveillance, kitchen appliance, computers, interact with various sensors and entertainment devices. HomeOS has a four layer architecture – the top of which is application layer, next is management

layer, then follows the device functionality layer and at the bottom stands the device connectivity layer. The HomeOS unifies various interface modules of the different devices and uses the C # language of the Microsoft.Net Framework 4.0 platform. There are also applications developed by Apple and Android phones and tablets that are used in home automation. Based on the forecast that this market will grow rapidly in the years to come, one can expect serious advances in home integration systems, devices and software.

Impact on society and challenges

Bearing in mind the presence of aging societies in the developed countries, it is very likely that one of the most important features of smart homes and factor that will push for their development and demand on the market is e-health/telehealth. Health services can benefit a lot in efficiency and quality when using advanced smart home features and implementations. Societies can improve quality of life for elderly and people with chronic conditions or disabilities, who wish to remain at home or do not have the opportunities to move to a specialized institution. Even simple automation like turning on/off lights when getting out of bed can facilitate better safety for those people. Meal intake, general activity, temperature, blood pressure, social interaction, communications and environmental hazards such as fire or gas leak are of paramount importance not only for the above mentioned categories of senior people or such with disabilities but also for children.

The major challenges with smart homes are the reliability of the sensors and surveillance systems, their calibration, provision of reliable communication from and to smart homes, granting security and integrity of data, provision of action plan or scenario in case of system failure or denial of services, security for the integration systems, including devices and decision taking software. In addition to the danger, related to the reliability and security, which are of technological and architectural design nature, there are also social dangers. For example, smart home inhabitants might feel social isolation from family and friends, or exert extra pressure on the older person who may feel unsafe [22].

SMART HOMES CYBER SECURITY CHALLENGES

With the introduction of smart devices and systems in our homes, the risks and threats linked to them, and respectively to the smart home inhabitants will grow. The digital world as we know it now has gradually developed standards, protocols, interfaces, operating systems, programming models and architectures during the last 50 decades, making both computing and networking a type of plug-and-play environment. The smart house and its services, as we know them at present, form a highly heterogeneous environment, which presents a significant challenge for future users and manufacturers. Healthcare services contain unknown so far danger for human's life. The scenario of a villain causing a heart attack by remote intervention in a pacemaker or shutting down an insulin pump on a diabetic is not in the realm of movies but occur due to real vulnerabilities that exist in connected medical devices [23]. These are rather worrying facts, bearing in mind that between 1993 and 2009, 2.9 million patients received permanent pacemakers in the United States with this number constantly increasing [24].

One definition of cyber threat is "any identified effort directed toward access to, exfiltration of, manipulation of, or impairment to the integrity, confidentiality, security, or availability of data, an application, or a federal system, without lawful authority" [25]. In our everyday life, a threat for our home can be an open window or unlocked door, an iron or cooker that are not turned off or water running from an open tap. In future smart homes, in addition to the threats related to the household appliance, there can emerge dangers directed to the health or life of the inhabitants.

Modern research shows that online cyber threats have not only grown and evolved considerably but have also expanded of traditional threats into new forums – social media, mobile devices and cloud computing [26], [27]. This territory will inevitably extend in the near future in smart homes.

CYBER THREATS CLASSIFICATION

The consequences of cyber attacks can lead to serious problems like misinformation, cripple tactical services, access sensitive information, espionage, data theft, financial losses, and other. The nature, complexity and severity of the cyber threats are increasing in time, which makes it difficult to build a good classification framework.

Cyber threats can be classified in several directions:

- According to the intention – unintentional and intentional. The cause of the former is due to lack of training, software upgrade, equipment failures or software upgrades that unintentionally disturb the functioning of computers or corrupt data. The latter can be either targeted or nontargeted.
    - Targeted attack aims at harming a person, institution or critical infrastructure system. Such may include the energy, finance, telecommunication, military, transportation or water sectors. They originate from spies, criminals, hackers, virus and malware programmers, or employees ("insiders") within an organization.
    - Non-targeted attack has no particular aim but is intended to do harm to as many digital systems as possible. Example of non-targeted attacks are viruses, worms, malware released on the Internet.
- According to the effect of the attack – critical, non-critical and non-critical but dangerous. Critical attacks can block or phase out entire systems, including infrastructural or certain modules, leaving them in limited or fully non-functional state. Non-critical attacks do not harm or modify the system or its elements. For example – classified information may be fetched; information to be used for marketing or advertisement purposes may be gathered. Non-critical but dangerous are such that do not cause immediate harm (no effect on the system or its elements) but may have critical effect at a later moment. For example – stealing passwords, identity theft, misuse of personal or confidential information, etc.
- According to utilization – syntactic and semantic. Syntactic attacks are direct – insert viruses, worms, malware, etc. Semantic attacks modify and/or disseminate information. Modified information can be used for covering tracks of crime, or setting somebody to a wrong track.

The recently published Red book - A Roadmap for Systems Security Research [28] presents the cyber security landscape of our society and lists the assets that are target of cyber attacks. The top four of them, which people feel are the most important are:

- Life – human's most valuable asset, which can be the target of cyber attacks. Such can be on medical systems, transport systems, emergency response systems all of which may lead to loss of life, even at some occasions – on a mass scale;
- Health – digital technologies are used in a larger scale, so is the increase of possibilities for cyber attacks on the health of individuals;

- The Environment – another asset, which is of paramount importance for the survival and healthy life of humans and all living species. Large scale pollutions, fires, or floods may have devastating effect on communities;

- Privacy – it is challenged even at the present state of society and appears to be even more threatened in the near future, as people are taking more and more actions online, their data and activities being recorded without their knowledge and control.

Security is fundamental for these four areas in order the development and future expansion of smart homes to be in line with people's most valued assets. So far there have been advances and big attention paid to securing communication protocols over Internet and for computer systems, but little is done in this respect for sensor technologies, integrated systems and smart home environment.

Table 1 presents the main services, dangers, critical attack points and consequences of cyber attacks in smart homes:

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.

Possible consequences from cyber attacks can be:

- Denial of service (DoS) – targeting the sensors, video surveillance or communication systems,
- Data integrity violation or data modification in communication media;
- System breach with unauthorized access to network resources or system integration resources.

To deal with the attack, it is necessary:

- to have an operating intrusion detection system;
- to have an attack prevention system;
- to maintain reliable identification, authentication and access control;
- to support leakage monitoring information;
- to employ reliable and effective communication protocols;
- to operate secure integrating systems and external communication systems.

Cyber threats modelling and identification

As the identification of cyber threats using experts' data could be performed in different ways, like: q-based surveys, discussions, morphological analysis, scenarios contextualization, etc., we have tried to find a more comprehensive method by implementing system modeling and analysis. This allows different data sources and analysis results integration and at the same time provides understanding of the threat's possible origin, thus marking the entities of interest. In the presented in Figure 2 model we have tried to integrate a q-based generated dimensions from a morphological analysis [29] into an E-R system model that is outlining the entities of interest of real/potential cyber threats.

Briefly, this methodological approach is based on the utilization of the well-known General Systems Theory, and thus concerns the studied system building elements in-between nonlinear interactions. An assumption for a smart home complex dynamic system approximation is made. It is built of entities and time-dependent weighted relations together with an improved graphical visualization of the entities' resulting sensitivity [30]. A more detailed description of the implemented software environment and resulting identified model entities classification is given in the next paragraph.

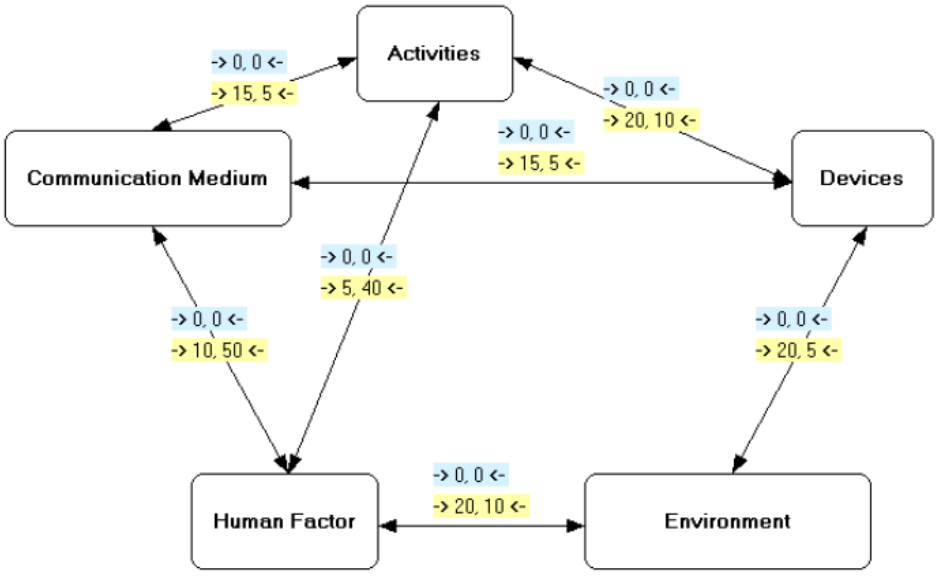

Figure 2. A smart home general system modeling for cyberthreats entities of interest identification.

Software implementation

The software environment model implementation is based on I-SCIP-SA v.2.0 [30]. Briefly, I-SCIP-SA allows models building by using "entities" (also noted as 'elements' or 'objects', interpreted as rectangles, squares or circles), which are connected with "bonds" ("relations", that are interpreted as headed weighted arrows – uni- and bi-directional). The arrows' weights are marked as yellow labels over the arrows and are expressed in percentages from the interval [0, 1] using the following scale: low [0-30], middle [30-50] and high [50-100].

The relations weights' generalization produce a Sensitivity Diagram (SD) that encompasses and extends the ideas of Vester's sensitivity model [31], allowing model entities' zone classification and system sensitivity analysis as follows: Red zone ('Communication Medium', active elements, Influence/Dependence Maximum Ratio (IDMR) =100/50, SE (South-East) part of SD cube), Blue zone ('Devices', 'Activities', passive elements IDMR=50/100, NW (North-West) part of SD cube), Yellow zone ('Human Factor', critical elements, IDMR=100/100, NE (North-East) part of the SD cube) and Green zone ('Environment', buffering elements, IDMR=50/50, SW (South-West) part of SD cube). Additionally, the 3D SD gives a possibility for direct sensitivity (z-coordinate, marked with red arrow in Figure 3) calculation of a given object from the system as an absolute difference between the influence (x-coordinate, marked with green arrow in Figure 3) and dependence (y-coordinate, marked with blue arrow in Figure 3) values, concerning a certain object from the system of interest. When this difference is negative the object in the SD is classified as passive (producing a decreased system sensitivity in its SD zone, 'Devices' and 'Activities') and is colored in light grey, otherwise it is active (producing an increased system sensitivity in its SD zone, all other model entities) and is colored in white.

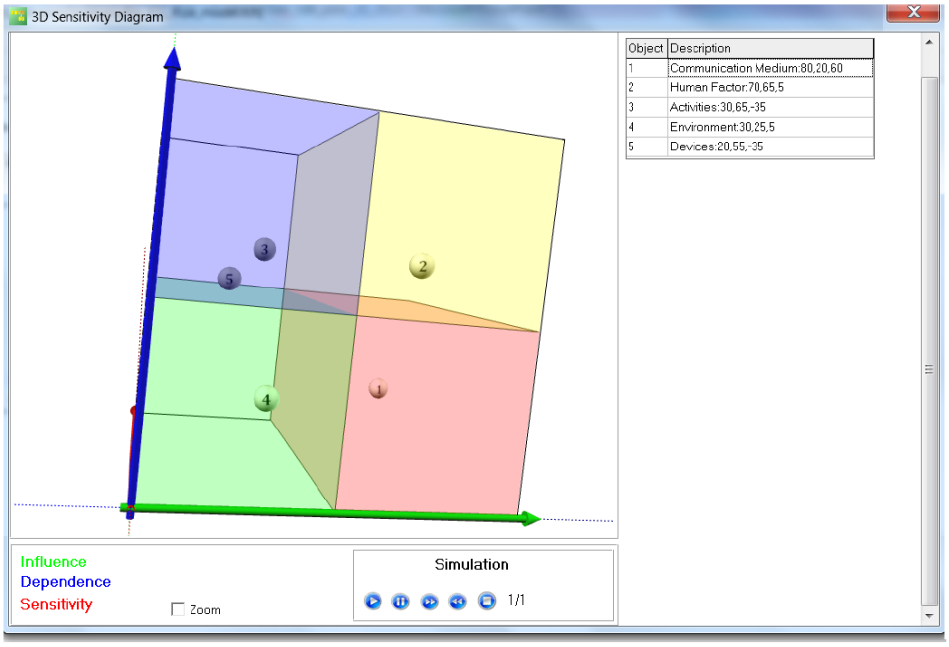

Figure 3. A smart home general system modelsensitivity diagram.

The resulting SD from Figure 3 is giving a profitable classification for further analysis, outlining the 'Human Factor'(noted in Figure 3 with indexed ball '2' with coordinates {x=70, y=65, z=5}) as a critical entity together with the potential hidden cyberthreats 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}). This expert' based classification, though quite general, is in line with a recently outlined comprehensive EU study of cyber security trends, developed by the SysSec international consortium [28].

As far as these results are based only on experts' data and analysis we have also decided to add a practical validation through a constructive smart home test bed simulation.

Results Validation

A suitable approach for experts' believes validation is the usage of a cyber-attacks simulation in a smart-home test-bed environment and monitoring human (smart homes' inhabitants) psychophysiological responses, as well as behavior dynamics to these attacks.

Agent-based modelling framework

Generally, the idea for interactive agent-based simulation could be summarized in Figure 4:

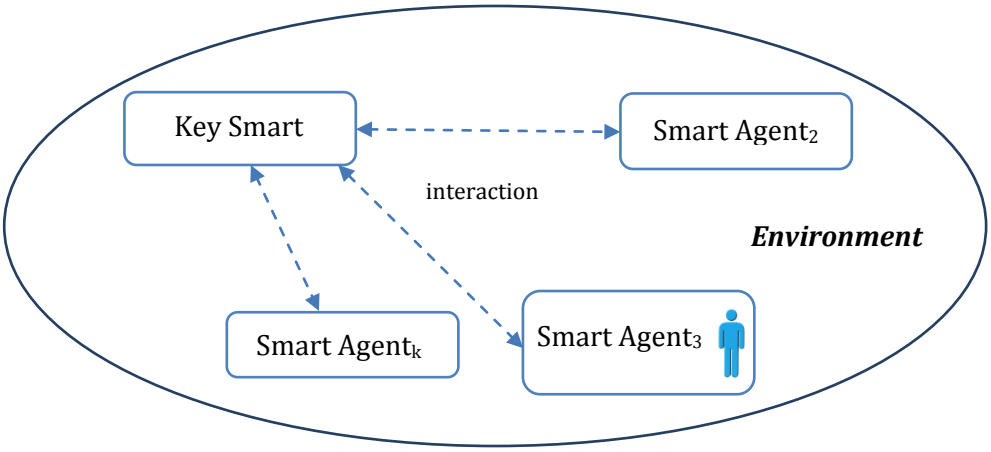

Figure 4. A general concept for interactive prominence agent-based simulation of cyber attacks in a smart home test-bed environment.

Figure 4 outlines the heterogeneous agent-based simulation concept with human-in-the-loop participation. As in general, no global organization of the model elements is required, two different swarm techniques could be used for autonomous multiagent-based interaction modelling: *prominence* and *negotiation* based organization [32]. For simplicity and fast practical smart home implementation, an assumption for prominence agent organization [33] is made, following the idea that each agent has two basic components: 'Properties' and 'Activities'. The 'Properties' set includes {*agent* ***role***, ***interaction channel***, *agent* ***state***, ***other*** *additional agent peculiarities*}. The subset ***other*** incorporates colour, weight, size, technical and environmental characteristics. When the agent role is presented by human, physiological properties are examined - heart rate variability, body temperature, galvanic skin response dynamics. When the agent role is given by smart room environment, physical parameters like environment temperature, humidity, CO concentration are monitored. The 'Activities' set covers the agent's behavior dynamics {**role dynamics**, **interaction events**, **state dynamics**}.

As the *prominence* swarm organization was chosen, the 'Key agent' is responsible for simulation running following a preliminary defined script of activities (noted in the 'Properties' and 'Activities' sets) covering different cyberattacks scenarios. More complex simulation configurations are also possible but require a busier communication channel and smarter agents.

Experimental test-bed

Recently, a smart home test-bed environment equipped with a number of smart devices, including: 3D TV/monitors, X-box game console, entertainment and cleaning robots, programmed tablet remote control, IP video omnidirectional monitoring system and digital assistant 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. The sensor barometer system will be extended with CO/CO2 concentration measurement, radiation, electromagnetic fields and dust particles sensors [34]. The bio headband is for ECG and body temperature monitoring [35]. All data from sensors and video monitoring is stored in data base storage. The above described test-bed has been organized for practical agent-based interactive experiments (see Figure 4) in the framework of DFNI T01/4 project [36].

Figure 4. A photo of experimental activities in smart home test-bed environment.

The simulation is currently based on a virtual agents' roles classification. A 'Key attacks agent' that is organizing cyber-attacks following a scenario script of events in cooperation with the 'Connectivity agent' is practically responsible for the simulation running. The other agents could be grouped according to their roles as follows: 'Data storage agent' (responsible for all exchanged data storing, encompassing at present environment and human biometrics sensors), 'Entertainment agent' (responsible for multimedia entertainments with audio-visual effects, social robots, intra/internet), 'Digital assistant agent' (providing voice, IR, Bluetooth remote control of smart room equipment), 'Monitoring agent' (encompassing all embedded sensor systems in the smart room), 'Connectivity agent' (organizing different communication channels routing and protection) and 'Human-in-the-loop agent' (a real human factor participant). All connections are organized via the 'Connectivity agent' through different protocols: Wi-Fi, LAN, Bluetooth, LAN, Xbee, IR and for the 'Human-in-the-loop agent' - audio-visual and multimodal biometric ones.

DISCUSSION

Modern smart homes have advanced significantly compared to those from the first half of the 20th century. This progress, however, has opened not only great opportunities and benefits, but also a number of threats to their inhabitants. Whilst some of these threats (classified in Table 1) look quite obvious, other related to entertainment, privacy and appliances (by means of emerging technologies) are hiding a number of unexplored domains. Examples for such new cyber threat areas are digital drugs (addiction to technologies) and social engineering that are especially important for the future generations of inhabitants of smart homes.

A suitable and promising framework approach for studying these problems is to combine experts' data, analysis, modelling, inhabitants and environment monitoring as well as practical validation through real experiments. This does not assure comprehensiveness, but at least provides plausibility of the near future technological progress and outlines measures to be taken it to account for their users.

REFERENCES

[1] Harper, R. (Ed), Inside the smart home, Springer-Verlag Publ., 264p., 2003, ISBN 978-1-85233-688-2.

[2] Kidd C, Orr R, Abowd G, et al., The aware home: a living laboratory for ubiquitous computing research. CoBuild'99, Proceedings of the 2nd international workshop on cooperative buildings, integrating Information, Organization, and Architecture, Springer-Verlag Publ., 191-198, 1999.

[3] Intille S, Larson K, Tapia M, et al.. Using a live-in laboratory for ubiquitous computing research, Fishkin KP, Schiele B, Nixon P, Quiley A, editors. Proceedings of the 4th international conference on Pervasive Computing, PERVASIVE 2006, vol. LNCS, Berlin, Heidelberg, Springer-Verlag Publ., 349–365, 2006.

[4] Helal S, Mann W, et al., The Gator Tech Smart House: a programmable pervasive space, Computer, vol. 38, issue 3, 50–60, 2005.

[5] Tamura T, Togawa T, Ogawa M, Yoda M., Fully automated health monitoring system in the home. Medical Engineering & Physics, vol. 20, No 8, 573–579, 1998.

[6] Matsuoka K., Aware home understanding life activities. Towards a humanfriendly assistive environment, ICOST'2004, Proceedings of the international conference on smart homes and health telematics, IOS Press, 186–193, 2004.

[7] Yamazaki T., Beyond the smart home, ICHIT'06, Proceedings of the international conference on hybrid information technology, 350–355, 2006.

[8] Bonner S., Assisted interactive dwelling house, Assistive Technology Research series, 6, IOS Press, Amsterdam, 524-533, 1999, ISBN: 1586030019.

[9] Cerni M, Penhaker M., Circadian rhythm monitoring in homecare systems, Proceedings of the 13th International conference on biomedical engineering, Vol. 23, 950-953, 2009.

[10] Chan M, Campo E, Esteve D., Assessment of activity of elderly people using a home monitoring system. International Journal of Rehabilitation Research, March, Vol. 28, No. 1, 69–76, 2005.

[11] Perez-Lombard L, Ortiz J, Pout C. A review on buildings energy consumption information. Energy and Buildings. s.l. : Elsevier Publ., Vol. 40, 394-398, 2008.

[12] A, Bae. www.navigantresearch.com/blog/articles/smart-house-in-japan. [Online]

[13] Research, ABI, https://www.abiresearch.com/press/15-million-home-automation-systems-installed-in-th. [Online]

[14] Chan M, Esteve D, Escriba C, Campo E. A review of smart homes - present state and future challenges. Computer methods and programs in biomedicine. s.l. : Elsevier, Vol. 91, 55-81, 2008.

[15] De Silva L, Morikawa C, Petra I. State of the art of smart homes, Engineering Applications of Artificial Intelligence, Volume 25, Issue 7, 1313-1321, October, 2012.

[16] Trankler H, Kanoun O, Recent advances in sensor technology, Instrumentation and Measurement Technology Confrerence, IMTC 2001, 309-316, 2001.

[17] Khoshnoud, F, De Silva, C, Recent advances in MEMS sensor technology – biomedical applications, Instrumentation and Measurement, Vol 15, No 1, 8-14, 2012.

[18] Fisher, J, 2006. Indoor Positioning and Digital Management: Emerging Surveillance Regimes in Hospitals. , Surveillance and Security: Technological Politics and Power in Everyday Life, New York: Routledge, 77–88, 2006.

[19] Hanshen G, Wang D., A Content-aware Fridge based on RFID in smart home for home-healthcare , 11th International Conference on Advanced Communication Technology ICACT 2009, Vol. 2, 987-990, 2009.

[20] Newitz A., The RFID Hacking Underground, http://www.wired.com/wired/archive/14.05/rfid.html [Online]

[21] Dixon C, Mahajan R, Agarwal S, Brush A, Bongshin L, Saroiu S, Bahl V, An Operating System for the Home, Microsoft Research – Publications, Microsoft, April, 2012.

[22] Borges I, Smart home: Independence or isolation for older people?, http://www.age-platform.eu/images/stories/EN/pdf_AGE_Presentation__Senior_project.pdf [Online]

[23] Computerworld, October 2012, http://www.computerworld.com/s/article/9232477/Pacemaker_hack_can_deliver_deadly_830_volt_jolt [Online]

[24] Greenspon A., et al, Trends in Permanent Pacemaker Implantation in the United States from 1993 to 2009, Journal of the American College of Cardiology, vol. 60, issue 16, 1540-1545, October, 2012.

[25] U.S. Department of Homeland Security, Privacy Impact Assessment for the Initiative Three Exercise 3, March 2010, http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_nppd_initiative3exercise.pdf [Online]

[26] Symantec Corp., Internet Security Threat Report 2013, Volume 18, http://www.symantec.com/content/en/us/enterprise/other_resources/b-istr_main_report_v18_2012_21291018.en-us.pdf [Online]

[27] Sophos, Security Threat Report 2013, http://www.sophos.com/en-us/medialibrary/PDFs/other/sophossecuritythreatreport2013.pdf [Online]

[28] 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]

[29] 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', at Grand Hotel "Sofia", Sofia city, Bulgaria, June 4, 165-169, 2013, http://smarthomesbg.com/files/dfni_t01_4_zm_lb_sg_paper_bulcip_proj_conf_june_2013.pdf [Online]

[30] 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.

[31] Vester, F. The Art of Interconnected Thinking, MCB Verlag GmbH, Munich, 2007.

[32] Minchev, Z. Generalized Nets Representation of Biological Inspired Multi-Agent Based Modelling, In Proceedings of BIOPS'05, Sofia, Bulgaria, October 25-26, III.81-III.94, 2005.

[33] A Conceptual Generalized Nets Immunological Model for Agent based Exploration of Unknown Environment, International Journal BIOAUTOMATION, 14(1), 49-60, 2010.

[34] 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, http://smarthomesbg.com/files/dfni_t01_4_sg_hk_no_el_paper_june_4_2013.pdf [Online]

[35] Georgiev, S., Minchev, Z. An Evolutionary Prototyping for Smart Home Inhabitants Wearable Biomonitoring, In Proceedings of Conjoint Scientific Seminar "Modelling and Control of Information Processes", Institute of Mathematics and Informatics, Sofia, Bulgaria, November 19, 2013 (in press), http://snfactor.com/snfactor/sites/files/sg_zm_paper_imi_19_nov_2013.pdf [Online]

[36] DFNI T01/4 Project Web Page, www.smarthomesbg.com. [Online]