The Eight International Conference on Business Information Security (BISEC-2016), 15th October 2016, Belgrade, Serbia

SM@RT HOME
PERSONAL SECURITY AND DIGITAL FORENSIC ISSUES

IGOR VUJAČIĆ
University Donja Gorica, Humanistic studies, Montenegro, vujacic@gmail.com

IVANA OGNJANOVIĆ
University Donja Gorica, Humanistic studies, Montenegro, ivana.ognjanovic.edu@gmail.com

RAMO ŠENDELJ
University Donja Gorica, Humanistic studies, Montenegro, ramo.sendelj@gmail.com

Abstract: *These days we are facing with expansion of off the shelf IoT solutions for SM@RT HOME. Recently, concept of SM@RT HOME has evolved from simple, separated, products for home automation into complex IoT systems for home monitoring, automation and security. Unfortunately, this rapid expansion was not followed by proper set of standards, especially in field of security and protection of system per se.*
This paper will take into consideration, and addressed some problems and open issues of personal security, and digital forensic challenges in that respect. It will show a possible solution through implementation of risk management cycle strengthened by digital forensic enablers like logging systems.
Finally paper will conclude that only proper level of awareness, accompanied by comprehensive advanced security intelligence concept can provide high level of personal security in SM@RT HOME environment.

Keywords: *Information Security, IoT, SMART Home, digital forensics, personal security, open standards, industry standards*

1. Introduction

Home was and still is much more than just an object for housing people, or place for living. Commonly, people will describe it as a nest, personal and family fortress, as a place where they can express themselves, but at the same time place where they are safe, secure and comfortable. They like to make it better, easier for day to day activities, modern, safe, secure, and comfortable, in order to improve life quality.

For the sake of improving life quality at home, SM@RT HOME concept emerged as a combination of new Internet of Things (IoT), and traditional devices and services [1].

The very first step on the SM@RT HOME road map was paved, in cyber realm time scale, long time ago. First, simple, home automation technology, called X10, was developed in 1975. Since then, end user demands grows from simple automation and controlling tasks inside house to comprehensive house security, monitoring, control and automation inside house and remotely. Those demands, over the years, dictated developing of different technologies and product lines for every single demanded functionalities, and lastly to converged them into complex SM@RT HOME system.

Paradoxically, even though lot of products was developed for home safety and security, those products does not implement proper level of security per se.

In developing of other SM@RT HOME product lines, security is low ranked if it is considered at all.

Those product are key carriers of our private information, and they have to have built-in support at least for identification, authentication and authorization (IAA), security audit, communication protection, and data encryption.

Unfortunately, legislative branch did not address this field properly yet, too. For instance, in EU there is no censuses about SM@RT HOME systems, predominantly caused by different cultures, economies and understanding of so called information societies. That is main reason why there are no dedicated EU policies covers IoT and SM@RT HOME [2].

Combination of those factors led us into the field of open opportunities for exploits SM@RT HOME system vulnerabilities in order to steal personal information, or to overtake monitoring and control over the home, and its inhabitants.

This paper will argue that only holistic approach to SM@RT HOME implementation will reach the aim to make our homes smarter, and our lives more comfortable. It will show the necessity for both, proper level of awareness, and implementation of active advanced security measures to mitigate cyber threats.

The paper is organized as follows: Section 2 gives the overview of SM@RT HOME concept evolution and expansion, Section 3 presenting security issues and

emerging threats landscape, and Section 4 proposing solutions to mitigate existing and upcoming threats. Section 5 concludes the paper summarizing recommendations and key findings.

2. Evolution and Expansion

The first well known and well spread technology for home automation is X10. It was developed in United States by Pico Electronic in 1975. Until now it becomes well accepted for home automation with more then million units.

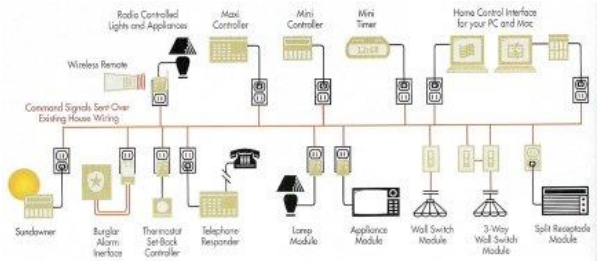

Image 1 - X10 schematic [3]

Recently, concept of SM@RT HOME has evolved from simple, separated, products for home automation into complex systems for home monitoring, automation and security. Today, we have a plenty of home automation and more advanced SM@RT HOME IoT products on the market. Some of them are regular industrial products, some of them are hobby and DIY kits. There are plenty of hobby platforms on the market [1, Chapter 1.3] [4]. The most popular DIY platforms for building SM@RT HOME are ARDUIONO [5] and Raspberry Pi [6]. The most popular open source project are OpenHUB [7] and Home Assistant [8]. For internal communication between devices different protocols were developed over time, like C-BUS, EnOcean, Insteon, KNX, Thread, Universal Power Bus, X10, xPL, Zigbee and Z-Wave. Some of them utilised power lines, some twisted pairs, Ethernet, RF spectrum or infra-red. Computing power of those devices vary from no computing functionalities to powerful devices.

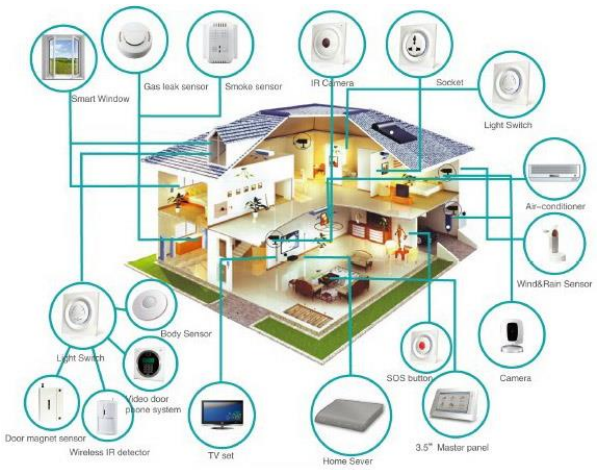

Image 2 - Modern SM@RT HOME system [9]

We can say today's SM@RT HOME is a melting pot of traditional real-time processing part of system: sensors, actuators, controllers, etc. and packet oriented part of system: most of IoT units and appliances, cameras, entertainment equipment, etc. of local Home Area Network and Wide Area Network, of local data, and cloud services and big data, and so on, like illustrated in images 2 and 3.

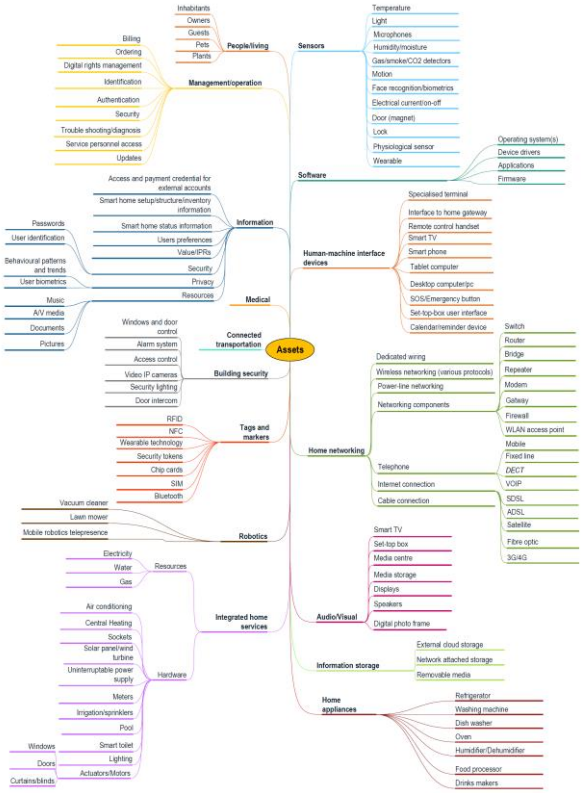

Image 3 - Overview of Smart Home and Converged Media Assets [10]

From both images, 2 and 3, we can conclude that beside traditional automation equipment, IoT devices plays a big role in today's SM@RT HOMEs. Proliferation of devices like wearables, smart thermostat, and similar

devices bring IoT into our Home Area Network (HAN). Those devices for their communication and management function utilise same communication infrastructure like traditional IT equipment.

In order to understand it better, we can split SM@RT HOME pot into ingredients and categorized them:

- by functionalities into [10]:
  - *Home automation and robotics*: lightening, HVAC, smart home appliances (smart refrigerator, dishwasher, washing machine), home robots (various assets starting from vacuum cleaner, autonomous grass trimmers and so on)
  - *Home monitoring and security*: video surveillance, gas leakage and flooding detections, fire detection and autonomous firefighting systems, burglar and access control system
  - *Health support systems*, as autonomous or as a part of larger health care system: different monitoring devices, and devices that monitor, control, and drive or correct human body functions
  - All other connected in home devices like: smart wearables, smart phones, tablets, computers, DVRs, receivers, set-top-boxes, streaming devices, game consoles, computers, and so on.

- by type of connectivity:
  - Wired,
  - Wireless long range,
  - Wireless mid-range,
  - Wireless short range.

- by interaction:
  - man 2 machine capable
  - machine 2 machine capable
  - hybrids

- by presence in Home Area Network
  - Permanently presented
  - Roaming between Home Area Network and external networks.

- by hardware (in [1], 2.1.2 Classes of IoT devices) on:
  - Constrained devices [11]:
    - class 0: simple sensors,
    - class 1: smart bulbs, smart locks, etc.
    - class 2: smart appliances and high-end smart sensors
  - High-capacity devices such as smart hubs/gateways and smart TV-s etc.

3. Security issues and emerging threats

When we are talking about security issues in general, network security is one of key issues targeting almost each application and system [12], aimed on preventing and monitoring unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources [13].

Many authors differently define key goals of network security [13] [14], while the following six goals are commonly used related to the topic of SM@RT HOME [15]: *Confidentiality*, *Integrity*, *Availability*, *Authenticity*, *Authorization*, *Non repudiation*; with definitions listed in Table 1.

Table 1. Network Security goals

Network security goal	**Definition/ description**
Confidentiality	The assurance that "data will be disclosed only to authorized individuals or systems" [14]
Integrity	The assurance that data will stay as is (unchanged) over time on storage, in memory or in transition over networks. Any modification or destruction should be recognised and logged.
Availability	The assurance that network resources will be ready (available) for processing any authorised requests and blocking unauthorised requests (attacks).
Authenticity	The assurance that communication actors really are who they claim they are, and the packets send from each one really belong to him, and is really emitted from him.
Authorization	The assurance that requested access rights by actors are matching with his assigned rights.
Non repudiation	The assurance that no one can deny what has been found as evidence.

Even the goals are clear, there is no unique approach to be applied for different systems and applications [16], and that is a reason why specific approaches and models shall be developed and applied. However, variety of factors should be considered [17]: architecture complexity, network topology, physical security, communication security, and lot more.

SM@RT HOME complexity is obvious. It is a mix and match of different type of technologies, devices, appliances, interfaces and protocols. Even though this complexity is problem per se, some additional problems are identified:

- Lack of open or industry standards to cover all aspects of SM@RT home. Despite the fact that lot of standards are developed, some guidelines and dedicated standards still missing, especially those

who will cover security issues properly [10, page 49].
- Vendors ether does not take a care about security, or make their own proprietary standards [1, Chapter 3.2]
- There are lot of cloud solutions for monitoring and control of our homes.
- Policy makers still does not have a consensus about SM@RT HOME, so there is a lack of laws and policies [2] [1 Chapter 8.5].
- Very limited knowledge and security awareness of end-users [10, Conclusions].

All those together are wide opened doors for personal security and digital forensic issues.

When we have bad planned, implemented or/and configure system, then we are exposed to both known and zero-day attacks. Significant problem, in ill configured system, is that we have no knowledge about security breaches. Once, when we finally became aware of it, then there are no logs and evidence that can be used for digital forensic to help us to figure out what was happened, what we have to face with, and what is damage scale. Within more complex systems this is even harder.

From a privacy aspect there are a lot of static (our first, last name, social security or identification number, data about credit card, day of birth, information about relatives, and everything else what was submitted somewhere or stored inside devices) and dynamic data(logs from devices or on-line collected data that represent our behaviour), stored inside our Home Area Network, or in connected cloud service that could be misused to make our digital profile (digital ID card), or to generate perfect ransomware virus, to perform fraud, etc.

Form a security aspect we are faced with additional serious problem, that SM@RT HOME can be used against us. Just imagine, possible, scenario when some hacker overtake control of our Home Area Network. Then he can monitor and read data from many different devices. By misusing our home monitoring and security system he can see what we are doing, when we are at home, how many of us, where we are inside home. So, he can track our habits and behaviours. Furthermore, he can take an action to lock up people inside, to change temperature, shut down ventilation system, close blinds, water, cut off power, and so on. As an extreme example, hacker can overtake control over our health care, and medical life support appliances and perform possible kinetic effect that will have direct implications to our life.

In the literature, many researchers and organizations [1], [10], [12], [13], [14], [15], [16], [17], [18], [19], [20], [21], [23] identified or/and addressed different kinds of potential threats and attacks for both, IoTs and SM@RT HOMEs. All agreed that identified issues having growing trends in recent time, and same forecast for upcoming period. Table 2 gives comprehensive view on security threats [10], possible attacks and scenarios [14] in relation to security goals previously defined in Table 1.

Table 2. SM@RT HOME security threats, possible attacks and scenarios

Security threats	**Security Goals Compromised**	**Possible attacks / scenarios**
Malware	All	Malware could be preloaded on device, or injected internally or externally.
Botnets (abusing IoT components as botnet nodes and/or C2 servers)	Confidentiality Availability Authenticity Authorization Non repudiation	Abused devices can attack other elements of SM@RT home, or could be abused for external attack.
Identity theft	Confidentiality Integrity Authenticity Authorization Non repudiation	Social engineering
Web based attacks	Confidentiality Integrity Availability	Spoofing DoS Information Disclosure Elevation of privileges …
Physical theft/damage/ loss	Confidentiality Integrity Availability	Physical stealing, accidental damage, remote control action
Phishing	Confidentiality Authenticity Authorization Non repudiation	By misusing using smart devices
Insider threat	All	By physical presence or by utilising some air interface
Information leakage	Confidentiality Authenticity	Apps and applets, ad-ware software

	Authorization Non repudiation	
Web application attacks	Confidentiality Availability Authenticity Authorization	By utilizing unblocked ports 80/443 to pass through firewall

4. Proposed solution

Lot of researches related to IoT security had be done so far, but not so many exclusively to SM@RT HOME security.
Bitdefender [18], Symantec [19], University of Michigan [20], and ENISA [1] [10] [21], for instance, took SM@RT HOME concept into consideration seriously, and published their research findings in research papers and periodic. In most cases, researches are focused on a few related issues, rarely to system overall.

It is really hard to address all those security threats and challenges. Only holistic approach to all aspects of SM@RT HOME, from design phase to the end of life cycle, can reach the aim to make our homes smarter, and our lives more comfortable, with simultaneously reduced risk of security breaches.

To reach that aim some prerequisites have to be fulfil:
- All stakeholders has to be actively involved in process.
- Policy makers and regulatory bodies has to change legal framework, and to adopt minimum requirements for standards, policies, guidelines etc.
- Industry has to be much more engaged in security (in making and introducing open standards), not only in upgrading functionalities and advertising of their products.
- Implementation and configuration has to be well explained as for dummies.
- End users has to be much more educated to be aware of security threats and their impact to their privacy, data, health and so on.

ISO/IEC 27001 [22] is good start in term of for risk management cycle. It covers planning an information security management system, risk assessment, and risk treatment. Additionally, well balanced combination of awareness, enforced with digital forensic enablers, like loggers, NextGen Firewalls [23], and trusted relation system can bring SM@RT HOME security to much higher level.

Unfortunately, most of SM@RT Home, and generally IoT industry argue there is no reason for implementation of advanced security in inexpensive products, like stated in [1]. They claim, that will raise up production costs and market price, and made products less affordable and less interesting. Furthermore, they still negate that IoT solutions including SM@RT HOME, are not targeted by hackers.

Some end-users argue there is no necessity for security measures implementation in Home Area Network, they ask for simplicity over security. They are refusing to learn how to configure system; they just like to have simple plug-and-play-and-forgot equipment. Those people does not take a care about privacy and security, either because they have lack of awareness, or they does not accepting at all that they can be a target of cyber-attack.

5. Conclusion

Even SM@RT HOME solutions are suddenly everywhere, security has been identified as important issue which is paying more attention by all, researchers, developers and native users. In this paper, we discussed SM@RT HOME solutions and identified key security issues, we also proposed key prerequisites to be fulfilled in developing new approaches and security models.

In addition to that, we conducted a review of recent literature on already identified security threats and possible attacks directly violating key security goals and principles. However, balance between simplicity and security should be maintained. SM@RT HOME solutions have to be planned, implemented and configure with that in mind. Only with this holistic approach SM@RT HOME will reach the ultimate aim to make our homes smarter, and our lives more comfortable with keeping security on desire level.

Acknowledgements. Research presented in this paper is conducted within the TEMPUS project 'Enhancement of Cyber Educational System in Montenegro (ECESM)', project no. 544088-TEMPUS-1-2013-1-SI-TEMPUS-JPHES.

REFERENCES

[1] ENISA, "SECURITY AND RESILIENCE OF SMART HOME ENVIRONMENTS, GOOD PRACTICES AND RECOMMENDATIONS", DECEMBER 2015, ISBN: 978-92-9204-141-0 | DOI:10.2824/360120

[2] THE EUROPEAN COMMISSION, "CONCLUSIONS OF THE INTERNET OF THINGS PUBLIC CONSULTATION ", PUBLISHED ON HTTPS://EC.EUROPA.EU/DIGITAL-SINGLE-MARKET/NEWS/CONCLUSIONS-INTERNET-THINGS-PUBLIC-CONSULTATION , AS ON AUGUST 31TH 2016

[3] PACIFIC CUSTOM CABLE INC. "X10 HOME AUTOMATION TUTORIAL"

HTTP://WWW.PACIFICCABLE.COM/X10_TUTORIAL_5.HTML

[4] JASON BAKER (RED HAT), "5 OPEN SOURCE HOME AUTOMATION TOOLS", ARTICLE, HTTPS://OPENSOURCE.COM/LIFE/16/3/5-OPEN-SOURCE-HOME-AUTOMATION-TOOLS

[5] ARDUIONO PROJECT HUB, "SMART HOME MINI ARDUINO – IN 30 MINUTES", PUBLISHED ON HTTPS://CREATE.ARDUINO.CC/PROJECTHUB/ANDREMENDES/SMART-HOME-MINI-ARDUINO-IN-30-MINUTES-POSTING-IN-UBIDOTS-224F0A

[6] "HOW TO BUILD A RASPBERRY PI SMART HOME", TUTORIAL, PUBLISHED ON HTTPS://WWW.PUBNUB.COM/BLOG/2015-08-04-TUTORIAL-BUILDING-RASPBERRY-PI-SMART-HOME-PART-1/

[7] OPENHAB FOUNATION , OPENHAB PROJECT HOMEPAGE HTTP://WWW.OPENHAB.ORG/, GitHub

[8] HOME ASSISTANT, OPEN SOURCE HOME AUTOMATION PLATFORM, HOMEPAGE, HTTPS://HOME-ASSISTANT.IO/ , GitHub

[9] SMART HOME ENERGY, LONDON, UK, "WHAT IS SMART HOME?", HTTP://SMARTHOMEENERGY.CO.UK/WHAT-SMART-HOME

[10] ENISA, "THREAT LANDSCAPE AND GOOD PRACTICE GUIDE FOR SMART HOME AND CONVERGED MEDIA", DECEMBER 2014

[11] INTERNET ENGINEERING TASK FORCE (IETF), "REQUEST FOR COMMENTS: 7228 - TERMINOLOGY FOR CONSTRAINED-NODE NETWORKS", MAY 2014, ISSN: 2070-1721

[12] R. J. ROBLES1, T. KIM, „A REVIEW ON SECURITY IN SMART HOME DEVELOPMENT", INTERNATIONAL JOURNAL OF ADVANCED SCIENCE AND TECHNOLOGY VOL. 15, FEBRUARY, 2010

[13] ANGUS WONG, ALAN YEUNG, "NETWORK INFRASTRUCTURE SECURITY", EBOOK, ISBN 978-1-4419-0166-8

[14] V. ARAVINTHAN, V. NAMBOODIRI, S. SUNKU, W. JEWELL, "WIRELESS AMI APPLICATION AND SECURITY FOR CONTROLLED HOME AREA NETWORKS," POWER AND ENERGY SOCIETY GENERAL MEETING, 2011 IEEE , PP.1-8, 24-29 JULY 2011

[15] KOMNINOS, N., PHILLPPOU, E. & PITSILLIDES, A. (2014), "SURVEY IN SMART GRID AND SMART HOME SECURITY: ISSUES, CHALLENGES AND COUNTERMEASURES.", COMMUNICATIONS SURVEYS & TUTORIALS, PP(99), DOI: 10.1109/COMST.2014.2320093

[16] R.ŠENDELJ, I.OGNJANOVIĆ, "SEMANTICALLY ENHANCED CYBER SECURITY OVER CLOUDS: METHODOLOGICAL APPROACH", INTERNATIONAL JOURNAL OF ADVANCES IN COMPUTER NETWORKS AND ITS SECURITY, 2014, VOL 4, NO.3, ISSN: 2250-3757

[17] TUHIN BORGOHAIN, UDAY KUMAR, SUGATA SANYAL, "SURVEY OF SECURITY AND PRIVACY ISSUES OF INTERNET OF THINGS", RESEARCH PAPER, HTTPS://ARXIV.ORG/FTP/ARXIV/PAPERS/1501/1501.02211.PDF

[18] BITDEFENDER, "THE INTERNET OF THINGS: RISKS IN THE CONNECTED HOME", RESEARCH PAPER, PUBLISHED FEBRUARY 2016

[19] MARIO BALLANOBARCENA AND CANDID WUEEST, "SECURITY RESPONSE; INSECURITY IN THE INTERNET OF THINGS" , RESEARCH PAPER, SYMANTEC, MARCH 2015

[20] EARLENCEFERNANDES, JEAYEON JUNG AND ATUI PRAKASH "SECURITY ANALYSIS OF EMERGIGN SMART HOME APPLICATIONS", RESEARCH PAPER, IN PROCEEDINGS OF 37TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY, MAY 2016

[21] ENISA, "ENISA THREAT LANDSCAPE 2015", JANUARY 2016

[22] ISO/IEC 27001:2013 "INFORMATION TECHNOLOGY - SECURITY TECHNIQUES - INFORMATION SECURITY MANAGEMENT SYSTEMS - REQUIREMENTS"

[23] PATRICK SWEENEY, "NEXT-GENERATION FIREWALLS: SECURITY WITHOUT COMPROMISING PERFORMANCE", ARTICLE, TECHREPUBLIC, HTTP://WWW.TECHREPUBLIC.COM/BLOG/IT-SECURITY/NEXT-GENERATION-FIREWALLS-SECURITY-WITHOUT-COMPROMISING-PERFORMANCE/