Development of a Multi-Vector Information Security Rating Scale for Smart Devices as a Means for Raising Public InfoSec Awareness

Stylianos Kavalaris\textsuperscript{a,b,*}, Fragkiskos-Emmanouil Kioupakis\textsuperscript{a}, Konstantinos Kaltsas\textsuperscript{a}, Dr Emmanouil Serrelis\textsuperscript{a,c}

\textsuperscript{a}AMC Metropolitan College, 74 Sorou st., Amaroussio 15125, Greece
\textsuperscript{b}Dixons South East Europe, 14km Athens Lamia NR, Metamorfossi 14452, Greece
\textsuperscript{c}ELPEN S.A, 14 Ag. Paraskevis st., Pikermi Attica 19009, Greece

Abstract

Vulnerabilities on smart multimedia devices that are made for homes and Small Office Home Offices (SOHO) and their implementation practices, are a pragmatic fact. The broad usage of various devices that operate in home and SOHO environments has introduced a new threat paradigm for consumer platforms and devices, aiming at the secure operation and information of home and SOHO networks. These devices include a wide variety of commercially available technologies required for their operation but also proprietary technologies tailored specifically for those devices. For many manufacturers, usability and user friendliness take precedence over the security on these implementations, leaving home and SOHO networks vulnerable to potential risks that are unknown to consumers or require deep technical knowledge to comprehend them. Poor implementations, along with the inheritance of vulnerabilities that already exist, aggravate these circumstances. This paper aims to construct a measurement method through known vulnerabilities and related attack methods, to provide a scaling system that helps end-users easily understand and be aware of each device’s vulnerability level, as well as provide a measurable score to help them compare devices that provide similar or identical services, in the same way this happens with other commodity features, attributes or characteristics.

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/). Peer-review under responsibility of Universal Society for Applied Research

Keywords: Information security metrics; information security quantification; information security rating; home and SOHO attack tree; smart devices; public awareness

* Corresponding author. Tel.: +30-694-4552121.
E-mail address: skavalaris@amcstudent.edu.gr
1. Introduction

Smart devices are already a part of life making the prediction for ubiquitous computing a reality. A lot of relevant studies and cases already exist, which prove that such devices have vulnerabilities that can be exploited using well-known attack methods and tools. The more devices and points of entry are created on a home or SOHO network, the more opportunities there are for an intruder to find a way in. In light of the importance in what these smart devices have access to and what security risks may pose, it’s important to find a way to inform end-users and ordinary people so that they understand their security risk. The methodology developed to serve one of the basic drivers of the paper, which is to raise the public awareness in terms of information security risks.

1.1. Smart devices definition

“Smart” is a word that is vastly overused these days for communication devices, appliances, home devices, residences and other buildings, as well as other types of devices and environments. The ability for the user to access the functions of an appliance or a device and monitor its status and settings from off-site, are most commonly linked to “smartness”. Smart devices and appliances have various definitions but in general they present abilities like sharing information with other devices and systems, integrate with applications using advanced APIs and accessing the Internet or a proprietary network. Smart devices also include a microprocessor and support the ubiquitous computing properties. The goal is to develop home/office appliance systems that allow these units to evaluate conditions and then communicate status condition with the consumer or other appliances. A smart home or SOHO environment can thus be defined as a residence, an office or other dwelling with automated or remotely controlled components (i.e. appliances and devices). Some “smart” components require a proprietary interface though most smart home features can be controlled by a mobile device or computer.

1.2. Common input and output media of smart devices

One of the most basic characteristics of smart devices are the input and output media. I/O media are the channels used from the device to interact with other devices or humans. Software-wise a communication can occur between a human and a machine using a user interface often provided by an operating system. Most commonly, but purely indicative, they include network interface cards such as wired Ethernet and Wi-Fi but also other types of wired and wireless media. Furthermore some smart devices incorporate other kinds of I/O media like sensors or other device-specific media. Each smart device uses a selected set of available I/O media required for the device’s operation. Individual media or specific combinations of certain media pose risks derived from vulnerabilities. Also implementation practices from device vendors may pose additional risks for some media or create risks for those that are relatively secure. The approach on these indicative I/O media depends on the concept that: It does not matter which exactly is the actual medium but how this can be categorized based on a vector class classification that is presented later on this paper.

2. Literature review

2.1. Information security rating methodologies

A number of assessment methodologies exist, each focused on different types of devices, based on a wide variety of parameters. A great amount of methods for risk analysis are without a complete assessment methodology and therefore produce no score. Other methods include the popular OWASP (i.e. risk-based), CVSS (i.e. metrics based), along with a small number of individual ones based on a variety of factors. Thus there is no specific methodology that can produce metrics and apply to such variety of devices, to date. The OWASP Risk Rating Methodology, follows the simple model “Risk = Likelihood * Impact”. OWASP provides flexibility for complex business models by adding new factors and calculating new varying weights for each new factor. The Common Vulnerability Scoring System (CVSS) is an open framework for describing vulnerabilities based on three groups (Base, Temporal and Environmental), apiece with various vectors. Each vector receives a variety of values and all the vectors are fed into
an equation to provide a score. The methodology focuses on the values of the respective vectors rather than providing a scale. A less popular methodology is the Threat Modeling method based on Attack Path Analysis (T-MAP). T-MAP quantifies security threats based on four metric, (namely Access, Vulnerability, Target and Affected Value to provide a score) and incorporates more business-oriented parameters which facilitate security management and potential software implementation. Furthermore, Microsoft’s Security Bulletin Severity Rating System, although a popular methodology, provides no score and is intended to inform all Microsoft users but in fact mainly enterprise customers reference it. Despite the wealth of valuable data each methodology provides, all are addressing IT security professionals and none inform with simplicity the end user. Furthermore other available methodologies and all previously analyzed, cannot evaluate the impact of unknown threats due to implementation flaws.

3. Scope of this paper

This effort aims to construct a novel information security measurement method that could inform end-users about the potential security issues that relate to specific commercial smart devices and also increase the level of information security awareness. This could be achieved through a simple visual indicator that could visually combine the joined risk for known as well as unknown vulnerabilities that could be applicable for that particular device. The scope of this research is to provide the foundations and parameters needed for the creation of a methodology that will lead to the standardization of measuring potential risk due to the usage of certain smart home and SOHO devices. This risk derives from already available vulnerabilities found in technologies used in those devices, potential vulnerabilities in generic technologies that vendors use, bad implementation practices or a combination of the above. Following the methodology, the standardized measurement will produce a scale that could potentially be used to evaluate each smart device. This scale could have the potential to be widely adopted by various parts of the smart device market such as the vendors themselves, end users/consumers and also by other areas.

4. Description and analysis of input vectors

By examining a vast number of smart appliances it has been concluded that these appliances and devices share common input vectors that are presented in detail on the following paragraphs.

4.1. Physical layer: Wireless

As per definition this paper focuses on commercial devices designed for end users, which can be interconnected with other devices. There are 3 different flavors of wireless standardized implementations found: Wi-Fi (802.11 a/b/g/n), Bluetooth and ZigBee all operating at 2.4GHz. There are also other implementations operating at higher frequencies such as 802.11ac or some implementations of 802.11n that operate at 5GHz, as well as other versions of the 802.11 standard that are not yet found in Smart Devices, that operate in various frequencies such as W1 Gig or White-Fi. Due to their nature that lacks physical connection all these implementations can potentially suffer from interference that can be emitted from numerous devices operating on the same band (e.g. wireless phones, for the 2.4GHz band), or specially crafted signal jammers, though the latter are illegal on most regions. Signal jamming usually renders the device temporary unavailable. Wireless radios can also be sniffed and cryptanalyzed resulting not only eavesdropping and information disclosure but also replay attacks and code injection.

4.2. Communication encryption

The Wi-Fi Protected Access and CCMP (WPA2) that is based in the strengthened AES encryption, has been proven the safest to date. Yet it can be forced if not applied correctly. All previous versions of Wi-Fi protections schemes were proven substantially insufficient and problematic. The Wi-Fi Protected Setup (WPS) standard that was added, from 2007 onwards, in order to provide an easy way for simple and safe interconnection of devices is erroneous by design as the predetermined 8-digit identification code (i.e. PIN) reduces the range of possible combinations, from 10 million to a mere 11.000 due to a design flaw. Also other erroneous designs similar to the WPS/PBC function were discovered, exposing protected networks with very little effort.
4.3. Network facilitators

With the term network facilitators we define all well-known traditional network protocols used in order not only for the devices to interconnect but also make installations easier for the end user by reducing manual configuration at a minimum level. Protocols like DNS and DHCP which are the most used can be found in smart devices with both Server and client roles. These protocols together with other protocols that are used in conjunction, such as ARP, or others used to ensure the network integrity, such as the STP which is being used to prevent network loops for devices with multiple network interfaces do not bear any security mechanisms by design and present inherent weaknesses not only by design but also if not implemented properly\textsuperscript{21,22,23}.

4.4. UPnP architecture

The UPnP architecture uses common technologies and protocols for both networking and Web in order to achieve usable and flexible connectivity, control and data transfer among UPnP enabled devices, thus interconnecting different electronic appliances and devices in an easy and effective way. According to research results\textsuperscript{24}, security flaws in UPnP-enabled network devices resulted the exposure of the SOAP API over the Internet and the exposure of more than 80 million devices via SSDP due to exploitable library versions. Also known attacks on both HTTP and XML\textsuperscript{25} prove that UPnP enabled appliances are potential exploitation points on a network.

4.5. File sharing and storage

Common Internet File System (CIFS) or Server Message Block (SMB) are the most common method of file sharing in smart devices. In fact CIFS is a form of SMB, but both terms are used for the file sharing protocol designed to allow devices to read and write files to a remote host over a local area network (LAN). Over the years there have been many security vulnerabilities either due to implementation of the protocol\textsuperscript{26} and lack of support for robust authentication protocols, in preference to no encryption or obsolete and already considered insecure\textsuperscript{27}. Thus SMB is considered one of the primary attack vectors for intrusion attempts\textsuperscript{28}. Web Distributed Authoring and Versioning (WebDAV) is another way of file sharing by extending the Hypertext Transfer Protocol (HTTP) so that it allows clients to perform remote Web content authoring operations, thus making the web a readable and writable medium. As an HTTP extension, attacks to WebDAV bear similarities to known web attack techniques\textsuperscript{29}. Storage devices can be used to exploit various vulnerabilities on smart devices such as deploying a modified firmware, a malware or another form of backdoor\textsuperscript{30}.

4.6. Console interface

The user interface console is the primary means of interaction between the users and the smart devices. Its purpose is to allow effective operation and control whilst providing information about the device, the service provided or other. These interfaces have identified design problems as 80 percent of devices raised privacy concerns (i.e. transmitting personal information unencrypted) and failed to require passwords of sufficient complexity and length, 70 percent did not encrypt communications to the Internet and local network and 60 percent raised security concerns with their user interfaces\textsuperscript{31}. As most interfaces are Web-based using html and JavaScript, common attack techniques like cross site scripting (XSS), cross site request forgery (CSRF), or using default and common credentials There are even cases where the console interface is hidden below a program or application for the user and no authorization process of any sort or use any credentials\textsuperscript{20}. Due to its nature the console interface can also be vulnerable to code injection. The above mentioned attacks can result multiple payloads such as Denial of Service, Disclosure of information, Arbitrary Code Execution or even full compromise of the device or appliance\textsuperscript{32}.

4.7. Operating system

Smart devices and appliances offer one or many services and in order to do so they operate under the control of an application specific or an embedded operating system. The vast spreading of the Android OS via smartphones
and tablets, lead to a branching out on media players and smart TVs but also more traditional home appliances such as fridges, cookers and washing machines. Many embedded Linux derives are also preferred by smart devices’ and appliances’ manufacturers. Of course there are also Windows and Apple iOS based devices as well as many clones of open source operating systems (e.g. WebOS) or scratch-built ones. Operating Systems due to their complexity often show security bugs, vulnerabilities and exposures due to erroneous applications, implementations or vulnerable libraries. An Operating System that is not patched to date may result a serious security breach. The embedded OSes that are designed to be compact, forsaking many functions that installable operating systems provide and can be found by the form of firmware created to cover specific hardware and task scope. 60 percent of such devices did not use encryption when downloading software updates, leaving them vulnerable to firmware manipulation.

4.8. Identified custom services and common practices

Apart from the traditional network services protocols and standards, modern features or transformation of older broadcasting methods initiate new industry standards and protocols, such as IPTV, HbbTV. Such initiatives found on commercial off-the-self devices, found to be built around html or java based solutions with concerns for implementations that are not tested thoroughly for security flaws or Software Of Uncertain Provenance (SOUP) that may compromise device safety. There are already published studies showing that these implementations may be attacked using the end smart device which is able to render Internet content. These implementations suffer also from Cross Script Request Forgeries because of their http based nature but also from erroneous implementations. Some common practices among vendors’ implementations also include the existence of hidden administrative accounts on the devices or remote reset procedures (e.g. opening a network port). These (mal)practices must also be addressed as they can be easily identified using common tools available on the internet and common techniques such as port scanning or brute-forcing.

4.9. The attack vectors’ methodology

There exist several classification methodologies and threat classification models that can be used to identify threat characteristics and attributes, implementation methods or resulting effects. The methodology of an attack tree is not only well known but already proved as very efficient, thus it can be used in combination with the input channels of particular smart appliances to build a master attack tree that can be used partially or fully on each tested subject according to its specifications and design, given the input vectors described earlier. The attack tree that can be formed using that information is shown in Fig. 1.

5. Methodology overview

Security rating sounds and is a very useful metric when it comes to a device intended for end-users. It is so far though, an abstract concept that cannot be measured or rated and thus expressed in a unique, simple and enlightening way. The rating methodology proposed on this paper is based on the quantification of measurable information security factors which are used as the input vectors. The motivation comes from the need to describe vague security issues based on various implementations with proper methodologies in a way that the result is expressed in a consistent, repetitive and comparable way that can easily inform an end-user about it, without the need of any expertise. The aim to build an objective information security rating scale for smart home and SOHO devices. In order to make the rating methodology meaningful to the public, a risk-based approach was selected. This approach is based on some measurable or objectively quantifiable items. These are vulnerabilities, implementation flaws and impact on the provided service. The rationale for choosing this methodology is that it has to specifically measure among common parameters and denominators and produce a realistic and understandable result. It is furthermore envisioned to apply an efficient way to identify the risk level of home or SOHO smart devices to the public without the assistance of security experts or consultants. Since every smart device has its own characteristics, the quantifiable items cannot be the same for all appliances. In order to identify the applicable items for each case, the “attack tree” methodology is used.
Fig. 1. The attack tree for smart devices.

The attack tree is built by identifying all applicable input/output media for the specific appliance. A list of potential input / output media (e.g. Wireless implementation, Interface, Networking facilitators, UPnP, Storage and file sharing, OS) was made through research and presented in the literature review. For each vector relevant attack scenarios are identified as well as their potential Vulnerabilities and/or Non-implemented Best Practices. By examining all vectors in combination with the applicable attack methods, the various scenarios that will develop, they will reveal vulnerabilities or non-implemented best practices and resulting payloads.

5.1. Methodology steps

When applying the methodology, the first step is to identify the I/O media for that particular smart device. In fact this translates into the medium vector of the attack tree. After identifying the I/O media, the next step is to build the attack tree that applies to that particular smart device. In the attack tree created, each of the main branches is based on the I/O media identified initially. The various applicable scenarios for each media vector should be identified creating minor branches each corresponding to a different scenario. Subsequently to that process, the methodology requires to identify the Potential Known Vulnerabilities (PKV) index from the CVE database. Each of the PKVs is then tested for the smart device in order to identify all Effective Vulnerabilities (EV) which in turn should be added to the attack tree, using a unique index number $i$ for each one. The Service Provision Impact ($SPI_i$), indexed uniquely as $SPI_i$, is identified for each one of the EVs, according to Table 2. The Total Applicable Vulnerability Rate ($TAVR$) is then calculated using the equation (1) where $i$ is the index number of the EV.

$$TAVR = \sum_{i=1}^{n} ES_i \cdot SPI_i$$

Table 2. Effective Vulnerabilities Service Provision Impact calculation.

| Impact on the Provided Service | Service Provision Impact |
|--------------------------------|--------------------------|
| No damage                      | $10^0 = 1$               |
| Temporal Non Availability      | $10^1 = 10$              |
| Permanent device damage        | $10^3 = 1,000$           |
| Loss/Leakage of data / sensitive data | $10^4 = 10,000$         |
| Human Injury or Death          | $10^6 = 1,000,000$       |
For the purpose of this paper the CIS-CAT\textsuperscript{41} seems more appropriate as an applicable information security best practice, due to the fast and easy installation and usage capabilities of the tool. An additional advantage is the large number of related metrics, such as “Mean Cost of Incidents” and “Risk Assessment Coverage” that the tool provides. Still, the selected tool set should be dealt as a dynamic “library” of best-practices, which selection is directly related to the specifics of each device. For each of the minor branches produced, the Applicable Non-Implemented Best Practices (ANIBP) needs to be specified. Each of the ANIBPs will then be added to the attack tree using a unique index number $j$ for each one.

The Probability Index ($PI$), uniquely indexed as $PI_j$ is specified for each one of the ANIBPs using the equation (2), where

- $E$ is the effort needed to exploit that particular ANIBP,
- $K$ is the level of knowledge needed to exploit that particular ANIBP, i.e. whether Programming and Network Skills are needed and
- $T$ is the availability of the tools needed to exploit that particular ANIBP.

$$PI_j = 1 + \frac{3}{2} \cdot \log(E_j \cdot K_j \cdot T_j)$$

The values of the $E$, $K$, and $T$ are set according to Table 4.

| Effort          | Knowledge | Tool               |
|-----------------|-----------|--------------------|
| High (>24h)     | $10^0 = 1$| Yes $10^0 = 1$     |
| Medium (1 to 24h)| $10^1 = 10$| No $10^2 = 100$ |
| Low (<1h)       | $10^2 = 100$| No tool $10^2 = 100$ |

The Service Provision Impact ($SPI$), uniquely indexed as $SPI_j$ for each one of the ANIBPs, is specified according to Table 6.

| Impact                          | Service Impact rate (points) |
|---------------------------------|------------------------------|
| No damage                       | $10^0 = 1$                   |
| Temporal Non Availability       | $10^1 = 10$                  |
| Permanent device damage         | $10^3 = 1,000$               |
| Loss/Leakage of data / sensitive data | $10^4 = 10,000$ |
| Human Injury or Death           | $10^6 = 1,000,000$           |

The Non Implemented Best Practices Rate ($NIBPR$) is calculated using the equation (3), where $j$ is the index number of the ANIBP.

$$NIBPR = \sum_{j=1}^{n} PI_j \cdot SPI_j$$

The total score ($MISR_a$ score) is calculated using the equation (4).

$$MISR_a = 10 - \log(TAVR + NIBPR)$$

Finally, the $MISR_a$ score is classified on the $MISR_a$ class from the $MISR_a$ score using Table 7.
Table 7. MISRa classification depending on the MISRa score.

| MISRa score | MISRa class | Class Description |
|-------------|-------------|-------------------|
| 9-10        | Class A+: 6 shields | Low likelihood for small number of threats that could cause “Temporal Non Availability” |
| 8-9         | Class A: 5 shields and 1 shield outline | Average likelihood for multiple threats that could cause “Temporal Non Availability” |
| 7-8         | Class B: 4 shields and 2 shield outlines | High likelihood for at least one threat that could cause “Temporal Non Availability” |
| 5.1-7       | Class C: 3 shields and 3 shield outlines | At least one threat that could cause “Permanent Device Damage” or multiple highly likelihood threats that could cause “Temporal Non Availability” |
| 4.1-5.1     | Class D: 2 shields and 4 shield outlines | At least one threat that could cause “Data Loss” or multiple threats with high likelihood that could cause “Permanent Device Damage” |
| 0-4.1       | Class E: 1 shield and 5 shield outlines | At least one threat could cause “Human Injury or Death” or multiple threats with high likelihood that could cause “Data Loss” |

5.2. Methodology output

The proposed methodology has been created to assist home users with evaluating a whole new generation of smart devices from the complicated perspective of security. Although smart devices vary in every possible manner, shape, purpose, I/O interface, connectivity etc., the goal remains the same, an easy reference to the security level of the device. To this end scales have been formulated, elaborate attacks have been estimated, security best practices have been assessed and many more steps as explained earlier. The previous statements prove that an average home user cannot appreciate or even understand the thinking behind this methodology and certainly should not.

6. Conclusions

6.1. Evaluation and future improvements

The paper’s aimed value was to suggest and prove a novel information security rating scale that could be used by both manufacturers and the public. Manufacturers could benefit from this method that objectively demonstrates the level of security achieved through their implementation and thus indicating their competitive advantage. The public could benefit from a simple means of recognizing quality products secured from common security threats. The offered level of simplicity could also act as a means to increase the commercial products information security. There exist researches\(^4\) that support the fact that the usage of security ratings, such the one presented in this paper, have subtle effects on service providers and customers respectively and increase the social welfare.

Assessing the efficiency of the proposed method, the objectivity level of the methodology results should be considered an aspect of paramount importance. It is therefore a definite advantage that most of the input vectors are well defined and thus objective. Still, few remaining aspects that may be seen having a more subjective nature can indicate areas of future improvement. These are the development of the attack tree and the identification of the various media, which may not be known in advance. Another topic of criticism can be the analysis and suggestion of a re-assessment process. Indeed, the number and type of threats that influence the implementation evaluation, as well as the attack surface at any given time, could change through the publication of new vulnerabilities or improved best practices. Hence, the frequency of re-assessment is quite important to reflect information security changing nature. Setting appropriate time intervals, could also benefit from additional research.

One more area of further analysis could be the confirmation of the chosen scaling ranges. The logarithmic scale used to calculate the final MISRa score was chosen for making harder to achieve scores greater than 8 but also quite easy to achieve scores greater than 4 as a manufacturers’ marketing-friendly approach. Another advantage of the proposed methodology is that can cover known and unknown threats and vulnerabilities. This particular aspect differentiates the MISRa methodology from others evaluated\(^7\,\,8\) and it is achieved through quantification of the implementation flaws through comparison with any chosen “best-practice libraries” (e.g. CIS). An additional
differentiating factor is the selected target group. Other methodologies focus on information security rating for enterprise infrastructures, whereas this paper focuses on information security rating for commercial products.

Considerations have been made regarding the entities that could reliably perform this methodology. Potential answers could include two certification phases. During the first phase only the methodology development team could perform such evaluations, ensuring consistency and objectivity. Any interested parties (vendors, customers or independent bodies) could communicate with the development team in order to apply and properly measure the security of any device. The second phase would expand the methodology usage to include standardized specifications to be used by any certified analysts, security product vendors, or application vendors in order to perform evaluations or self-evaluations through this methodology. Moreover, any parties interested to become certified, could submit an application to the methodology development team, providing the requested technical and procedural evidence required. The interested parties should also agree to adhere to all terms and conditions set by the team for any rating performed using MISRa. Future expansions could also use a broader range of best practices such as DISA – NIST\textsuperscript{43}, OWASP\textsuperscript{44}, SANS\textsuperscript{45}, CSA\textsuperscript{46}, adopted in the aforementioned order, which is based on the variety of the suggested security practices as well as their adoption difficulty. Finally additional input vectors and media could also be considered, analyzed and used to include cloud connectivity, voice control, as well as various sensors in order to accommodate the evolution of smart devices connectivity capabilities.

6.2. Synopsis

Current methodologies for information security rating have been found to be inadequate when used for raising the public awareness regarding the threats and risks related to smart devices. This paper presented a novel methodology for rating smart devices information security that could be used as the foundation for raising public information security awareness, as well as a marketing tool for manufacturers. While information security is seen as a complicated technical issue by most consumers, the proposed methodology manages to provide a simple and comprehensive way to understand and present the risks involved in the usage of any smart device. Moreover, it could also provide a visualized version to the underlying technical issues that could be understood by end users so that they will be able to compare smart devices from information security perspective. Technically oriented individuals will also have access to the bare technical aspects of each device. The earned value of this research was the incorporation of implementation flaws, through the evaluation of non-implemented best practices, with any known vulnerabilities, through the usage of updated databases. These features are much more significant for evaluating consumer smart devices than enterprise products, where there is much more awareness and technical skills to support the related process. Adopting this methodology could provide any industry related to smart-devices to take advantage of a new marketing tool, increase the quality of their products, through raising their information security level. Consumers and independent bodies could also benefit by raising the overall information security awareness and thus enabling the mitigation of a wide variety of threats that exist in current devices. This paper strongly supports its educational purpose to create information security and privacy awareness and training programs but also as a form of implicit learning.

References

1. A. Greenfield, "Everyware: The dawning age of ubiquitous computing", New Riders, pp. 11-14, 2006.
2. Hewlett Packard, "Internet of Things Research Study," July 2014. Available: http://h30499.www3.hp.com/hpweb/attachments/hpweb/application-security-fortify-on-demand/189/1/HP_IoT_Research_Study.pdf.
3. George Wilkenfeld and Associates, "Appliances Get Smart:But how and when?," 25 February 2014. Available: http://www.clasponline.org/~/media/Files/SLDocuments/2014/2014-02_Appliances-Get-Smart.ashx.
4. B. Dragt, "Universal Commerce: Adapting to the Power of Smart Devices," First Data Corporation, 2012.
5. S. Poslad, "Ubiquitous Computing," in Ubiquitous Computing: Smart Devices, Environments and Interactions, Wiley, 2009, pp. 75-78.
6. J. Rutenbeck, in Tech Terms, Elsevier, 2006, pp. 193-194,227-228.
7. OWASP, "OWASP Risk Rating Methodology," OWASP, 19 September 2014. Available: https://www.owasp.org/index.php/OWASP_Risk_Rating_Methodology.
8. P. Mell, K. Scarfone and S. Romanosky, "A Complete Guide to the Common Vulnerability Scoring System Version 2.0," June 2007. Available: https://www.first.org/cvss/cvss-guide.pdf.
9. Y. Chen, B. Boehm and L. Sheppard, "Value Driven Security Threat Modeling Based on Attack Path Analysis," in 40th Hawaii International International Conference on Systems Science (HICSS-40 2007), Waikoloa, Big Island, HI, USA, 3-6 January 2007.
10. Microsoft, "Security Bulletin Severity Rating System," May 2012. Available: https://technet.microsoft.com/en-us/security/gg309177.aspx.
11. IEEE Computer Society, "Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band," in Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, New York, USA, IEEE, 28 December 2012.
12. D. Lekomtev and R. Maršálek, "Comparison of 802.11af and 802.22 standards," electorevue, vol. 3, no. 2, pp. 12-18, 2012.
13. T. Schroeder and M. Moser, "Practical Exploitation of Modern Wireless Devices," 2010. Available: http://www.remote-exploit.org/content/keykeriki-v2-demo-src.zip.
14. B. Stelte and G. D. Rodosek, "Thwarting Attacks on ZigBee," 9th CNSM and Workshops, pp. 219-226, 2013.
15. M. Bellare, J. Killian and P. Rogaway, "The Security of the Cipher Block Chaining Message Authentication Code," Journal of Computer and System Sciences, Volume 61, Issue 3, pp. 362-399, 2000.
16. A. Tsitroulis, D. Lampoudis and E. Tsekleves, "Exposing WPA2 security protocol vulnerabilities," International Journal of Information and Computer Security Volume 6 Issue 1, pp. 93-107, 2014.
17. A. H. Lashkari and M. M. Danesh, "A Survey on Wireless Security protocols (WEP, WPA and WPA2/802.11i)," Computer Science and Information Technology, ICSIT 2009. 2nd IEEE International Conference on, Beijing, IEEE, pp. 48-52, 2009.
18. E. Tews and M. Beck, "Practical attacks against WEP and WPA," in WiSec ’09 Proceedings of the second ACM conference on Wireless network security, 2009.
19. S. Viehböck, "Brute forcing Wi-Fi Protected Setup Version 3," 2011.
20. S. Kavalaris and E. Serrelis, "Security Issues of Contemporary Multimedia Implementations: The Case of Sonos and SonosNet," in The Proceedings of the International Conference in Information Security and Digital Forensics, Thessaloniki, Greece, 2014.
21. K. Lauerman and J. King, "DHCP Consumption Attack and Mitigation Techniques (white paper)," Cisco Press, 2010. Available: http://www.cisco.com/c/en/us/products/collateral-switches/catalyst-6500-series-switches/white_paper_C11_603833.html.
22. Y. Bhaiji, "Understanding, Preventing, and Defending Against Layer 2 Attacks," Cisco, 2007. Available: http://www.nanog.org/meetings/nanog42/presentations/Bhaiji_Layer_2_Attacks.Pdf.
23. G. Kambourakis, T. Moschos, D. Geneiatakis and S. Gritzalis, "Detecting DNS amplification attacks," in In Critical Information Infrastructures Security, Springer Berlin Heidelberg, 2008, pp. 185-196.
24. H. Moore, "Security Flaws in Universal Plug and Play," RAPID7, 2013.
25. A. Chuvakin and C. Peikari, "Chapter 15. SOAP XML Web Services Security," in Security Warrior, O'Reilly, January 2004, pp. 228-233.
26. J. M. Johansson, "How to Shoot Yourself in the Foot with Security, Part 1," 8 September 2005. Available: https://technet.microsoft.com/en-us/library/cc512612.aspx.
27. US-CERT, "Alert (TA14-353A) Targeted Destructive Malware," 19 December 2014. Available: https://www.us-cert.gov.
28. M. Pangaria, V. Shrivastava and P. Soni, "Compromising windows 8 with metasploit’s exploit," IOSR Journal of Computer Engineering (IOSRJCE), vol. 5, no. 6, pp. 01-04, 2012.
29. Rapid7, "Microsoft IIS WebDAV Write Access Code Execution.," Available: http://www.rapid7.com/db/modules/exploit/windows/iis/iis_webdav_upload.asp. Accessed January 2015.
30. Z. Wang and A. Stavrou, "Exploiting Smart-Phone USB Connectivity For Fun And Profit.," in ACSAC ’10, Austin, Texas USA, 2010.
31. OWASP, "OWASP Internet of Things Top Ten Project," OWASP, June 2014. Available: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_Ten_for_2014.
32. OWASP, "OWASP Top 10-2013," The OWASP Foundation, 2013.
33. L. Xing, X. Pan, R. Wangy, K. Yuan and X. Wang, "Upgrading Your Android, Elevating My Malware:Privilege Escalation Through Mobile OS Updating," Security and Privacy (SP), 2014 IEEE Symposium on, pp. 393-408, 2014.
34. C. Hobbs, "Industry Viewpoint: Device makers can take COTS, but only with clear SOUP," 11 November 2011. Available: http://medicaldesign.com/prototyping/industry-viewpoint-device-makers-can-take-cots-only-clear-soup.
35. Y. Oren and A. D. Keromytis, "From the Aether to the Ethernet—Attacking the Internet using Broadcast Digital Television," Proceedings of the 23rd USENIX Security Symposium, pp. 353-368, 2014.
36. Y. Oren and A. D. Keromytis, "Attacking the Internet using Broadcast Digital Television (white paper)," Columbia University, 2014.
37. E. Vanderbeken, "How Sercomm saved my Easter!," 18 4 2014. Available: http://www.synacktiv.com/ressources/TCP32764_backdoor_again.pdf.
38. W. Ahmad, Z. Hayat, B. Zafar, F. Khan, F. Din and I. Shah, "A Survey on Taxonomies of Attacks and Vulnerabilities in Computer Systems," International Journal of Computer Science and Telecommunications Volume 3, Issue 5, pp. 93-97, May 2012.
39. B. Schneider, "Ch. 21 - Attack Trees," in Secrets & Lies: Digital security in a networked world, Indianapolis, USA, Wiley Publishing Inc, 2004, pp. 318-333.
40. E. Serrelis and N. Alexandris, ""Measuring Network Security," in Radio Communications, Rijeka, Croatia, InTech, April 2010, pp. 673-687.
41. Center for Internet Security, "CIS-CAT and Other CIS Benchmark Assessment Tools," Center for Internet Security. Available: https://benchmarks.cisecurity.org/downloads/audit-tools/. Accessed February 2015.
42. Z. Z. Zhou and E. M. Johnson, "The Impact of Information Security Ratings on Vendor Competition," in AMCIS 2009 Proceedings. Paper 280, 2009.
43. National Institute of Standards and Technology, "National Checklist Program Repository.", Available: http://csrc.nist.gov/standard/nist.SP.800-53/ assessment/.
44. Open Web Application Security Project Foundation, "OWASP Testing Guide v4," 2014. Available: https://www.owasp.org/images/5/52/OWASP_Testing_Guide_v4.pdf.
45. SANS Institute, "CWE/SANS TOP 25 Most Dangerous Software Errors," 27 June 2011. Available: http://www.sans.org.
46. Cloud Security Alliance, "Sampling of issues we are addressing," 2009. Available: https://cloudsecurityalliance.org/issues.html.