Proc. 14th Int. Conf. on Global Research and Education, Inter-Academia 2015
JJAP Conf. Proc. **4** (2016) 011615

Home Communications and Services with Enhanced Security: Augmented Embedded Systems for Communication Appliances as an Educational Platform

Kamen Kanev[1,2], Alessandro Mei[2], and Paolo Bottoni[2,1]

[1]*Graduate School of Science and Technology, Shizuoka University, Japan*
[2]*Department of Computer Science, Sapienza University of Rome, Italy*

E-mail: kanev@rie.shizuoka.ac.jp

(Received September 25, 2015)

The increased dependence on ICT services makes home users more vulnerable to online attacks, security breaches, identity thefts, and unauthorized access to valuable information if specific measures and precautions are not properly instated. Nowadays, wired communications are giving way to wireless, and most of the computing devices and appliances that we use are always online, hence potentially vulnerable to attacks and unauthorized access. We address such security issues by an embedded solution targeting home users and small home networks that could be employed on a wide range of communication hardware (e.g. home routers) as a replacement of the standard manufactures firmware. The design, development and all practical aspects of the integration of such embedded system solutions into existing communication appliances are considered as essential components of the Embedded Systems academic course with hands-on experience and practice on networking that we build.

1. Introduction

Information and communication services are an essential part of our daily life. The increased exposure to, and dependence on, ICT services makes us more vulnerable to online attacks, security breaches, identity thefts, and unauthorized access to valuable information if specific measures and precautions are not properly instated. We enjoy the security of our homes behind securely locked doors but are our "communication doors" to the digital ICT world out there equally secure? As wired communications are giving way to the wireless and most of the computing devices and appliances we use are always online, we become potentially vulnerable to attacks and unauthorized access.

Computing and communication safety should be considered from both the technological and the psychological points of view. Highly secure professional solutions such as IBM Security Network Protection XGS [1], CISCO Integrated Network Security Architecture [2], and others are readily available for enterprise customers, albeit too complex and prohibitively expensive for private use. Communication services providers, however, are obliged to provide all their customers with adequate means for information security management and control as part of the communication and computing services they provide to end users. In most cases, for example, home users subscribe with an Internet provider and lease or buy a router from it as part of a service package. Such routers are sometimes configured for centralized control and management by the service provider, overriding local controls available to the end user. This may be a good feature since it reduces the burden and responsibilities of the end user, but it may also become a serious security issue if the master control retained by the provider is hijacked.

We believe, therefore, that there is a need for specialized low-cost solutions targeting home users and small home networks with more flexibility and control to be delegated to the end users while still maintaining network security at an elevated level. Our approach is to provide an embedded system solution that could be employed on a wide range of readily available commercial communication hardware such as network routers, access points, and other appliances for small business and private users. The design, development and all practical aspects of the integration of such embedded system solutions into existing communication appliances are envisaged as essential components of an Embedded Systems academic course with hands-on experience that we build.

2. Communication Appliances in Educational Environments

Our research and corresponding student projects as discussed in this work focus on embedded systems for communication appliances and related security issues. We see those as essential steps and a milestone on the way to a specialized educational environment for teaching and practical work with embedded systems for engineering and computer science students that we build. More details on how our current work integrates in this concept are provided in the following sections.

2.1 Embedded System platforms

While introductory Embedded Systems (ES) courses are included both in the Engineering and Computer Science programs, their scope is greatly limited due to program time constraints. There is a need for more advanced and practically oriented courses of a wider scope that could be offered to students from different backgrounds. Such ES courses should allow for hands-on experience on the design and implementation of integrated ES solutions including both software and hardware.

By definition an ES is a computing system with a dedicated function that is embedded as part of a device or as a component of a larger electronic system. Indeed, embedded systems are all around us- they control almost every home appliance we use and they are in all of our gadgets such as audio players and recorders, still and video cameras, etc. We have a lot of hands-on experience with such appliances and gadgets, but how much do we know about the embedded systems that drive them? Learning about embedded systems and developing relevant practical skills require a different kind of hands-on experience. For this purpose, we need an educational setup that would allow for deeper exploration of both hardware and software and that should be suitable for both engineering and computer science students.

While any device driven by an embedded system could be considered as a potential educational platform for engineering students that put more stress on the hardware, computer science students would benefit more if the device and its embedded system are not studied in isolation but as components of a larger communication framework that integrates different embedded devices. Although many home appliances are being enabled with communications, it would take some time before a communication framework of embedded systems that controls standard appliances such as microwave ovens or refrigerators could be adopted as an educational platform. But for embedded systems that control communication appliances like network gateways, routes, and wireless access points, etc. such an integration is part of their natural mode of operation.

Based on the above we deem communication appliances to be particularly suitable as an embedded systems platform in respect to the requirements that we have outlined. Note that such communication appliances have already been used for teaching Computer Networks in real networks [3] and as inexpensive Linux routers in hands-on network laboratory setups [4, 5].

2.2 Communication appliances hardware and respective firmware

Nowadays many home router producers employ common chipsets and other hardware components that can be successfully operated by open source firmware to ensure more compatible interfaces which are easier to learn and to operate. While different community projects are currently engaged in developing and building such multiplatform firmware for home routers and other communication appliances, in this work we focus on the two most common ones, namely the DD-WRT [6] and OpenWRT [7, 8]. In fact one of the major home router producers in Japan, Buffalo [9], has already brought to market a limited number of home router models controlled by the DD-WRT professional firmware, which is a development effort of the router producer that uses the standard DD-WRT community firmware as a starting point.

The interface and functionality of the community DD-WRT firmware have not been adopted in full in the professional firmware, so its users are facing various interface discrepancies and incompatibilities. However, the system we have designed is based entirely on the community version of the DD-WRT firmware and is thus able to provide a uniform interface and compatible functionality across a large span of hardware platforms from Asus, Buffalo, D-Link, Linksys, Netgear, TP-Link, and others. Some DD-WRT compatible network appliance models are listed in Table I.

Table I. DD-WRT compatible network appliance models.

Producer	Model
Buffalo	BHR-4GRV, WBMR-G300, WCR-GN, WHR-1166D, WHR-300HP2, WHR-600D, WHR-G300NV2, WHR-HP-G300N, WHR-HP-GN, WLAE-AG300N, WLI-D1300, WXR-1900DHP, WZR-300HP, WZR-300HP, WZR-1166DHP, WZR-1750DHP, WZR-300HP, WZR-600DHP, WZR-600DHP2, WZR-900DHP, WZR-D1100H, WZR-D1800H, WZR-HP-AG-300H, WZR-HP-AG-300NH, WZR-HP-AG-300NH2, WZR-HP-AG-301NH, WZR-HP-AG-450H
Linksys	E1700, E2100L, EA2700, EA6300, EA6400, EA6500, EA6500V2, EA6700, EA6900, WRT160NL, WRT400N, WRT1200AC, WRT1900AC, WRT1900ACV2, WRT54G2V11
Netgear	AC1450, EX6200, R6250, R6300, R6300V2, R6700, R7000, WR302V1, WG302V2, WNDR3700, WNDR3700V2, WNDR3700V4, WNDR3800, WNDR4300, WNDR4500, WNDR4500V2, WNR2000V3, WNR2200, WGT624V2

3. System Design and Implementation

3.1 System organization

We have attempted to design and implement our system following some typical user home communication patterns. In a standard setup a single Internet provider contract may service just a single user within the limits of an individual room or a small apartment or may span to a large family living in a multistory house. In both cases multiple devices such as smart phones, tablets, notebooks, TV sets, desktop computers, and other networked home appliances are likely to be used simultaneously and thus interconnected to form a home communication network. Such a home network is usually centered around a routing device, typically with Wi-Fi capabilities, that also serves as a gateway to the Internet. The home router is often the single access point for all communication devices and networked appliances at home so it is of utmost importance in regard to networking and communication security. Enhancing the security of a wireless home router is two-fold: it has to take into account the security of the gateway to the Internet as well as the wireless access point [10]. While standard security techniques such as firewalls and encrypted Wi-Fi access are readily available, their proper roll-out and enforcement often become problematic in home environments where professional support is more limited.

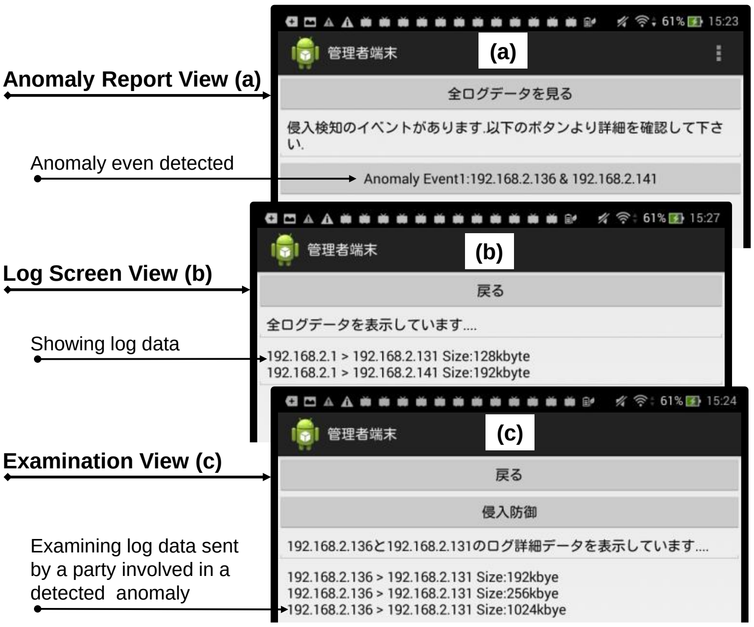
Home communications security management, when delegated to a home user, is prone to misuse and potential security breaches due to improper setup and lack of consequent follow-up and control. The problem is further aggravated by the lack of unified standards for home router setup and management which leads to the proliferation of many largely incompatible interfaces as provided by different hardware makers with their proprietary firmware.

The system that we are developing consists of a set of software modules that integrate with the DD-WRT firmware. It allows for the installation of Optware packages from OpenWRT and enhanced security features specifically designed for non-professional users. This includes extensive logging and real-time notifications of critical situations and potential security breaches. The system also features a security console implemented as an Android application that allows simplified secure access for critical router setup and management.

3.2 Implementation results

An experimental implementation of the proposed enhanced security system has been carried out as a student graduation research project. As such, one of our educational objectives was to provide basic knowledge and ensure hands-on training in Embedded Systems Development. The router security project made an excellent exemplary case where participating students invested significant time and effort to learn the specificities of multiplatform development environments with cross-compilers for different chipsets. The resulting enhanced security code developed by the students was successfully cross-compiled and integrated with the pre-installed DD-WRT firmware on a WRZ-600DHP Buffalo Wi-Fi router.

Students were also encouraged to learn about secure communications and to implement a secure console for interacting with the embedded router firmware. Android Studio and SDK Tools were used to implement the console application which was run on an Android Smartphone as shown in Fig.1. In the final experimental setup the code embedded in the rooter firmware monitored different security aspects of the router and communicated in real-time with the secure console application installed on the Android Smartphone.



侵入検知のイベントがあります.以下のボタンより詳細を確認して下さい.

Anomaly Event1:192.168.2.136 & 192.168.2.141

全ログデータを表示しています....

```
192.168.2.1 > 192.168.2.131 Size:128kbyte
192.168.2.1 > 192.168.2.141 Size:192kbyte
```

192.168.2.136と192.168.2.131のログ詳細データを表示しています....

```
192.168.2.136 > 192.168.2.131 Size:192kbye
192.168.2.136 > 192.168.2.131 Size:256kbye
192.168.2.136 > 192.168.2.131 Size:1024kbye
```

Fig.1. Implemented secure console application running on an Android Smartphone.

In a network setup, embedded systems of communication appliances practically never work in isolation. Even a simple home router as the one we have used in our experiments integrates in a communication framework of a gateway, communication hubs, and various wired and wireless appliances some of which belong to the embedded system educational platform that we are developing. This allows us to initiate student projects for different network appliances that will ultimately work together in a concerted way which provides for a better understanding of key embedded system concepts and thus increased educational value.

4. Conclusion

We see this experimental embedded system implementation for enhanced security of home communications and services as a proof of concept that is paving the way for the design and development of more advanced approaches. We are, therefore, planning to continue our research in this area elucidating the adopted concepts for home communications and services with enhanced security and expanding the experimental base to include routers from different makers and based on different chipsets.

Acknowledgment

This work was supported in part by funding for exchange of researchers provided by the Ministry of Foreign Affairs of Italy, funding for a Cooperative Research Project at Research Institute of Electronics, Shizuoka University, and KAKENHI Grant 25560109. We thank the anonymous reviewers for the useful comments, which helped improve the paper.

References

[1] IBM, Beyond the Next Generation: Putting Advanced Network Security to Work, EMA White Paper, November 2012.

[2] J. Oltsik, Integrated Network Security Architecture: Threat-focused Next-generation Firewall, ECS White Paper, September 2014.

[3] Pan, J., Teaching Computer Networks in a Real Network, SIGCSE'10, March 10-13, 2010, Milwaukee, Wisconsin, USA, pp.133-137.

[4] Heldenbrand, D., Carey, C., The Linux Router- An Inexpensive Alternative to Commercial Routers in the Lab, JCSC 23, 1 (October 2007), pp.127-133.

[5] Jasani, H., Vendor Neutral Nands-on Labs using Open=Source Products for Wireless Networks Courses, The 40th ASEE/IEEE Frontiers in Education Conference, Washington, DC, USA, October 27-30, 2010, pp.S3F1-6.

[6] DD-WRT. URL: http://www.dd-wrt.com/, Retrieved July 2015.

[7] OpenWRT. URL: https://openwrt.org/, Retrieved July 2015.

[8] Palazzi, C., Brunati, M., Roccetti, M., An OpenWRT Solution for Future Wireless Homes, IEEE ICME 2010, pp.1701-1706.

[9] BUFFALO. URL: http://www.buffalo-technology.com/en/technology/partnered-software/dd-wrt/, Retrieved July 2015.

[10] Tsow, A., Jakobsson, M., Warkitting: The Drive-by Subversion of Wireless Home Routers, Journal of Digital Forensic Practice, 1:179-192, 2006.