2016 IEEE International Conference on Computational Science and Engineering, IEEE International Conference on Embedded and Ubiquitous Computing, and International Symposium on Distributed Computing and Applications to Business, Engineering and Science

Design of a secure BYOD policy for the Greek School Network: a Case Study

Vasileios Gkamas
Computer Technology Institute and
Press "Diophantus", Rio, Greece
vgkamas@cti.gr

Michael Paraskevas
Computer Technology Institute and
Press "Diophantus", Rio, Greece and
Technological Educational Institute of
Western Greece, Antirio, Greece
mparask@cti.gr

Emmanouel Varvarigos
Computer Technology Institute and
Press "Diophantus", Rio, Greece and
National Technical University of
Athens, Athens, Greece
manos@ceid.upatras.gr

***Abstract*—The proliferation of mobiles devices, such as laptops, tablets and smartphones, has led a number of educational networks to define Bring Your Own Device (BYOD) policies that allow students and teachers to bring their own devices to school and use them for educational and learning purposes. This paper presents a case study for the design of an effective and secure BYOD policy for the Greek School Network, discussing also the main security challenges and issues faced and how they were handled. We believe that BYOD is a promising technology that could add long-term value in the educational process and learning activities, when it is designed in a secure and efficient manner.**

Keywords— Bring your own device, mobile devices, security, educational networks, Greek School Network

I. INTRODUCTION

Internet access over mobile devices has exhibited a steady and rapid growth during recent years, a trend which is expected to continue in the future. In particular, according to "Ericsson Mobility Report" [1], the users' subscriptions for Internet access through mobile devices have been increased exponentially, with smartphones being the most often used devices for mobile Internet access. Furthermore, according to a survey conducted by Online Publishers Association [2] on the use of tablets in the USA, 15% of the respondents declared that they use their tablet from their office or school, for work and educational purposes, respectively, while according to the "Cyber Security" survey [3] conducted on behalf of the European Commission, 30% of the respondents declared that they use a smartphone or tablet for Internet access. Therefore, the use of mobile devices is not limited only in house covering personal needs (such as communication and entertainment), but it is also extended to other places, including work, university and school, covering additional needs (such as working and learning).

In this context, there is a growing pressure to let mobile devices owned by individuals, such as employees in an organization or students in a school, to access corporate resources (network, data and services) in an effective and secure manner. The emerging Bring Your Own Device (BYOD) policy [4] addresses this need by defining the strategy and policies for accessing corporate resources over personal devices. The adoption of a BYOD policy within an organization raises various challenges and issues; a great deal of work has been performed on security issues that arise in connection to BYOD policy [5-9], while many other works have focused on the design of BYOD programs for educational purposes [10-13]. However, despite of the challenges and risks that raise by the adoption of a BYOD policy, a lot of benefits also exist. In the case of an educational environment (network) these benefits are outlined as follows: (a) strengthening of students' personalized learning, (b) easier access to digital educational content, (c) increase of teachers' and students' productivity and satisfaction, and (d) important cost savings and increase in the return of ICT investments.

In this work, we present a detailed framework for the design and implementation of an effective and secure BYOD policy in the Greek School Network (GSN). In the case of GSN, the need for the adoption of a BYOD policy is re-enforced by the "Digital School" strategy, a strategic plan established by the Greek Ministry of Education (MoE), in order to modernize the primary and secondary level educational system in Greece, through the exploitation of innovative ICTs. Actions that have been implemented in the context of the "Digital School" strategic plan, like the development of digital educational content and its effective distribution, and actions planned, like the installation of mobile computer laboratories and interactive whiteboards in schools, make imperative the design of a BYOD program in the GSN for educational and learning purposes.

Although the proposed BYOD framework was designed for the case of GSN, it is general enough and can be re-used with minor adaptations by any other organization (not necessarily of educational character). Given that security is a key challenge faced by a BYOD policy, especially in an educational network as students (and teachers) are its main users, we also describe the main technical issues and challenges we faced from a security point of view and the way they were handled. Our work extends previous works, by proposing a rather complete framework for the design and implementation of a secure and effective BYOD policy in an educational network, covering both technical and operational issues.

The rest of the paper is organized as follows. Section II describes the Greek School Network. The proposed framework for the design of the BYOD policy in Greek School Network is described in Section III, while the main security issues and challenges faced during the design of the BYOD policy are discussed in Section IV. Finally, Section V concludes the paper.

978-1-5090-3593-9/16 $31.00 © 2016 IEEE
DOI 10.1109/CSE-EUC-DCABES.2016.241

II. GREEK SCHOOL NETWORK

The Greek School Network [14], [15] is the educational intranet of the Greek Ministry of Education. It interconnects all schools, educational administrative offices, public libraries and general state archives in Greece and it also provides advanced e-services to its users (students, teachers, schools, etc.). The Greek School Network is operated and supported by a consortium of twelve universities and academic institutes, under the coordination of Computer Technology Institute and Press "Diophantus". It is the biggest national public network in Greece in terms of number of users, and it has been recognized internationally as a remarkable educational network which promotes the introduction and exploitation of ICTs in the Greek educational system.

GSN offers to its users a novel ICT-based environment suitable for the realization of modern educational methodologies and the adoption of modern practices, as the services provided have been designed to appeal to the profile of all GSN users. The services provided are categorized as follows: (a) basic services (broadband network connectivity, users' registration, GSN portal, etc.), (b) communication services (e-mail, instant messaging, video-teleconference, live webcasting, etc.), (c) e-Learning services (asynchronous e-learning and e-portfolios, learning activity management system, etc.), (d) collaborative services (collaborative documents, social networking with blogging, microblogging and content curation, etc.), (e) central infrastructure services (Domain Name System, Lightweight Directory Access Protocol, Single Sign On, etc.) and (f) management services (network monitoring and security, remote administration of school IT labs, etc.).

The majority of schools is connected to GSN through ADSL/ADSL2+ circuits, while a considerable number of schools is connected through optical fibers. With regards to the local area networks installed at schools' labs for the interconnection of IT equipment (personal computers, server, printer, etc.), the majority of them are implemented as wired local area networks using the IEEE 802.3 protocol (Fast Ethernet or Gigabit Ethernet networks), while a small number of them are implemented as wireless local area networks, using the IEEE 802.11 protocol (Wi-Fi networks).

III. BYOD DESIGN FRAMEWORK

In this section, we describe the proposed design framework of BYOD policy for the case of GSN. The main requirements defined for the design of the BYOD policy are the following:

- Heterogeneity. This requirement ensures that the users will be able to access the GSN network (and the provided services), regardless of the type of mobile devices used and the type and version of OS installed.
- Interoperability. This requirement ensures that all the services (e.g. GSN services, repositories hosting digital educational content) provided by MoE will be interoperable with users' mobile devices.
- Equal accessibility. The solution designed ensures the equal accessibility of all students to the provided services, so that all students will be able to participate in the ICT-based learning activities (using their mobile devices) with common means.
- Extensibility. The solution designed will be extensible in an effective and cost efficient manner, in order to deal with increased number of users, or new services.
- Security. The solution designed ensures the protection and integrity of data and the confidentiality and privacy of users (students, teachers and schools).

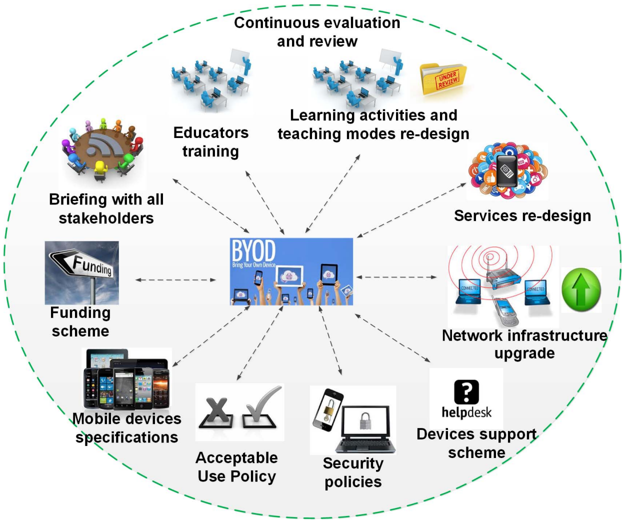
Continuous evaluation and review
UNDER REVIEW
Educators training
Learning activities and teaching modes re-design
Briefing with all stakeholders
Services re-design
BYOD
Bring Your Own Device
Funding
Funding scheme
Network infrastructure upgrade
Mobile devices specifications
Acceptable Use Policy
Security policies
helpdesk
Devices support scheme

Fig. 1 Proposed BYOD design framework

The implementation of the BYOD policy started with a pilot phase with the participation of few schools. From the pilot phase, useful conclusions were derived with regards to the educational added value of BYOD model, and the processes that must be revised in order to improve its effectiveness. The continuous evaluation and review of the BYOD policy is important for its sustainability and its effective exploitation in the implementation of educational and learning activities. The BYOD design framework (Figure 1) defined in the case of GSN, includes the following ten steps:

- Step 1: Briefing with all stakeholders. The first step towards the implementation of a successful BYOD policy is to inform all stakeholders about it. In the case of an educational network, such as GSN, indicative stakeholders are the educational directorates, the parents, the school directors, the teachers, representatives of IT industry, etc. The goal of this step is to highlight the benefits that will be reaped in terms of cost and improvement of educational process, by adopting the BYOD policy and to remove any concerns for its implementation.
- Step 2: Determine funding scheme. At the second step, the funding scheme for the procurement of the IT mobile devices has to be investigated. The funding scheme that will be selected can decisively influence the degree of success of the BYOD policy. Possible funding schemes are the following: procurement of devices by the MoE, procurement of devices by each school, procurement of devices by teachers (or parents in the case that students

will be also allowed to bring their own devices at schools) and procurement of devices by teachers (or parents) by providing to them a subsidy.

- Step 3: Definition of mobile devices' specifications. During this step the minimum specifications of the mobile devices are defined. The specifications must cover both software and hardware aspects, like the type of mobile device (laptop, smartphone, tablets, iPad, etc.), the operating system installed (iOS, Android, Microsoft Mobile, Blackberry, etc.), the software installed, the network interfaces, etc.

- Step 4: Definition of Acceptable Use Policy (AUP). For the effective and secure implementation of the BYOD policy, various critical parameters have to be defined in the context of an AUP: which users will have access to the school network's resources, which applications the users will have access to, etc. The policies defined must be clear and accurate in order to ensure users' and especially students' security and the security of network, data and services.

- Step 5: Definition of security policies. Another critical issue, is the definition of the security policies governing the BYOD program. Indicative issues that must be defined by the security policy are the following: how the physical security of the devices will be ensured, how the users will be able to access the school network, what type of security software will be installed on the devices (antivirus, firewall, parental control), etc. In every case, only authorized users and devices must have access to school network resources.

- Step 6: Definition of mobile devices' support scheme. In this step the devices' support scheme in terms of installed hardware and software has to be defined. In the case of GSN, a hybrid helpdesk service is operated which provides support through telephone or Internet and on-site support when this need arises. This hybrid model could also operate for the case of BYOD policy. Special care must be taken in order to ensure that the mobile devices will be supported after the expiration of their warranty, in case of hardware malfunctions.

- Step 7: Network's infrastructure upgrade. The adoption of a BYOD policy in a school network, especially when students are involved, has as a consequence a remarkable increase in the network traffic. Therefore, the necessary actions must be carried out in order to update the network infrastructures at the level of both access and distribution network. This includes the installation of wireless networks and modern broadband routers at schools, the broadband upgrade of schools access to GSN, etc. The solutions applied must be scalable and cost effective in order to ensure their sustainability and extensibility.

- Step 8: Services re-design. At this step, the necessary changes must be made to the electronic services provided, to make them accessible through mobile devices, like smartphones and tablets. This need is addressed by the "responsive web design" principle which in the case of web pages, concerns not only the design of them but also their content (hierarchical structuring of information, definition of important content, content availability, etc.).

- Step 9: Learning activities and teaching modes re-design. The use of IT mobile devices for educational purposes introduces a new educational and learning environment, implying that learning activities and teaching modes, such as Blended Learning model or Project Based Learning model, have to be re-designed. This is necessary in order to effectively promote the comparative advantages of BYOD over traditional lecture-dominant teaching methods.

- Step 10: Teachers' training. The last step of the proposed BYOD design framework focuses on teachers' training on new educational scenarios and learning activities using the mobile devices. This is of critical importance for the BYOD policy in order to be universally and successfully accepted by the educational community.

Note that the proposed design framework is general enough and can be re-used by any other organization with minor adaptations (in order to address specific needs) for the implementation of a BYOD program.

IV. BYOD Security Issues And Challenges

In this section we focus on the main security issues and challenges faced during the design of the BYOD policy. These issues include users' authentication, separation of personal and school data, and mobile devices' management.

A. *Users' Authentication*

One major security issue we faced during the design of the BYOD policy was users' authentication. Although wireless local area networks have been installed on a pilot basis in a few schools, an easily deployable, scalable and cost-effective users' authentication mechanism has to be defined.

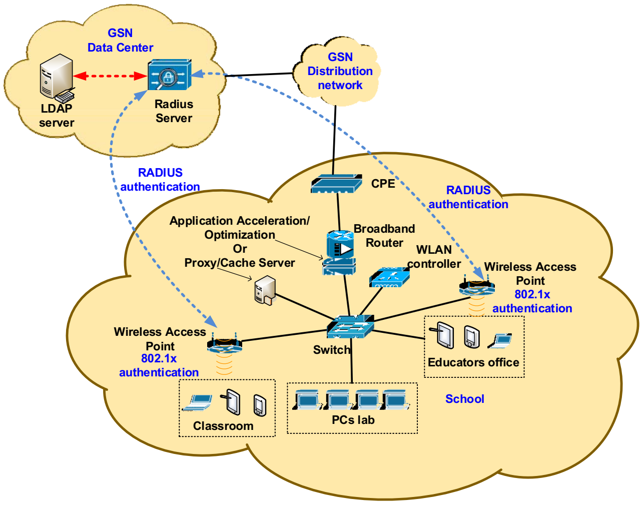

Fig. 2 Mobile users' authentication.

Users' authentication includes two phases: in the first phase the user must be authenticated in order to access the school wireless network, while in the second phase, the user must be authenticated in order to access the GSN network and its services. To cover the aforementioned needs we propose the use of IEEE 802.1X authentication mechanism for authenticating the users to access the school wireless network, and the use of a RADIUS server using LDAP for authenticating the users to connect to GSN, by providing their credentials to a captive portal.

The proposed authentication mechanism is depicted in Figure 2. When a user wants to connect to GSN through a mobile device, the following procedure is followed. The user is asked to provide the required credentials in order to connect to the wireless network. If the credentials are correct, the user is successfully authenticated by the 802.1x authentication mechanism and is connected to school's wireless network. When the user tries to open a web page, the HTTP request is redirected to a captive portal, where he/she is asked to provide his/her GSN credentials in order to connect to the GSN network. The user provides his/her personal credentials, which are forwarded to the RADIUS server. In the case of successful authentication, the user is connected to GSN, otherwise he/she is asked to provide again his/her GSN credentials.

The captive portal can be incorporated at each access point firmware, or to a wireless access controller that controls a set of access points. We must note that the broadband router installed at school will operate as a DHCP sever for providing IP addresses to mobile devices, a service that is already provided to desktop PCs.

B. *Separation of personal and school data*

Separation of personal and school data is another security issue that must be handled very carefully in a BYOD policy. An efficient and secure BYOD policy must separate school and personal data on devices (such as e-mail, GPS location, personal user information, etc.), through customizable privacy policies that are based on device ownership type. Mobile devices must conform to the security policies governing their access to the school network, while at the same time personal data must also be protected. This challenge becomes more important when students are allowed to bring their own devices to school in order to avoid unwanted sharing of personal data to the Internet. Solutions like mobile device management platforms can be used in order to ensure personal and school data separation and safety. The BYOD policy must also allow schools to mitigate risks that are presented when user-owned devices are accessing corporate resources. Custom Terms of Use agreements based on user role, organization group and device platform inform users about what data will be captured and what they are allowed to do with the device.

C. *Mobile Device Management*

Mobile devices' management [16] is another security issue that needs to be addressed by a BYOD policy. There are a lot of commercial and open source solutions, named Mobile Device Management (MDM) platforms that cover this need. Although users loose part of their flexibility with the use of a MDM system, such systems provide a lot of functionalities for device management, like automated device provisioning, enforcement of devices security policies, remote management of mobile devices, provision of reports and analytics, etc. Additional benefits of using a MDM platform include budget's reduction for devices' support (as the devices can be centrally managed by the MDM) and increased security, ensuring that the mobile devices are maintained according to organization's standards for protecting the corporate resources and data integrity standards.

V. CONCLUSION

We proposed a framework for the design of an effective and secure BYOD policy for the Greek School Network, addressing both technical and operational aspects. Furthermore, we discussed the main security challenges and issues that appeared during the design of the BYOD policy and the way they were handled. We believe that BYOD is a promising policy that through its secure and effective design, can play a beneficial role in the educational process, by providing a versatile environment suitable for the realization of ICT-based modern educational methodologies and learning activities.

REFERENCES

[1] Ericsson, "Ericsson Mobility Report", 2012.

[2] Online Publishers Association, "A Portrait of Today's Tablet User - Wave II", 2012.

[3] European Commission, "Cyber Security Report", 2012

[4] J. Keyes, "Bring Your Own Devices (BYOD) Survival Guide", Florida: Auerbach Publications, 2013.

[5] Y. Wang, J. Wei, K. Vangury, "Bring your own device security issues and challenges", IEEE 11th Consumer Communications and Networking Conference, pp. 80-85, 2014.

[6] K.W. Miller, J. Voas, G.F. Hurlburt, "BYOD: Security and Privacy Considerations", IT Professional, Vol. 14, No. 5, pp. 53-55, 2012.

[7] A. Scarfò, "New security perspectives around BYOD", 7th International Conference on Broadband, Wireless Computing, Communication and Applications, 2012.

[8] A. Armando, G. Costa, L. Verderame, A. Merlo, "Securing the Bring Your Own Device Paradigm", Computer, Vol. 47, No. 6, pp. 48-56, 2014.

[9] S. Misun, L. Kyungho, "Proposal of MDM Management Framework for BYOD use of Large Companies", International Journal of Smart Home, Vol. 8, No. 1, pp. 123-128, 2014.

[10] I. Pogarcic, M. Markovic, V. Davidovic, "BYOD: A challenge for the future digital generation", 36th International Convention on Information & Communication Technology Electronics & Microelectronics, 2013.

[11] Y. Son, "Bring Your Own Device (BYOD) for seamless science inquiry in a primary school", Computers & Education, Vol. 74, pp. 50-60, 2014.

[12] K. Sangani, "BYOD to the classroom", IET Engineering & Technology, Vol. 8, No. 3, pp. 42-25, 2013.

[13] N. B. Sardone, "Making the Case for BYOD Instruction in Teacher Education", Issues in Informing Science and Information Technology, Vol. 11, pp. 191-201, 2014.

[14] Greek School Network, http://www.sch.gr/aboutsch/english.

[15] M. Kalochristianakis, M. Paraskevas, E. Varvarigos, N. Xypolitos, "The Greek School Network, a paradigm of successful educational services maturing based on open source technology", IEEE Transactions on Education, Vol. 50, No. 4, pp. 321-330, 2007.

[16] K. Rhee, W. Jeon, D. Won, "Security Requirements of a Mobile Device Management System", International Journal of Security and Its Applications, Vol. 6, No. 2, pp. 353-358, 2012.