Results of implementing WPA2-Enterprise in Educational Institution

Konstantin Yanson
SPO Faculty
ITMO University
Saint-Petersburg, Russia
k-yanson@corp.ifmo.ru

Abstract — **This article devoted to practical results of implementing wireless access to an educational network for students end employees in the SPO department of the ITMO University during 4 educational years. Experimental result shows how users deal with security whilst using their BYOD. Security and simplicity are two desirable but incompatible features that need to be balanced. Paper can help to find trade-off between security and convenience when we implement WPA2-Enterprise authentication. Results show what happens when we put security on users and at the same time cutback IT supplying.**

Index Terms **— BYOD, WPA2-Enreprise, MSCHAPv2, educational network.**

I. Introduction

This paper discusses the findings of the survey results pertaining access to the wireless network in the SPO department of the ITMO University during 2012-2016 years. ITMO University is an acknowledged leader in IT and quantum technologies in Russian Federation and in the world. It enters the top-100 QS BRICS rankings. The SPO department provides secondary special education in areas: “Programming in computers systems” “Information systems in economic”, “Computer networks” and “Automatic control systems”. The graduates are highly demanded in different areas of IT. The SPO department provides program of uninterrupted continuous professional education. It means that graduates continuing study on the 2nd or 3nd level of higher education (bachelor). The department works with students in different ages, providing uninterrupted educational program. [1][12]

The use of mobile devices in education and work environment is constantly increasing. It had brought new challenges for IT departments since BYOD (Bring You Own Devices) students come to educational institutions. Intel coined the BYOD term in 2009 and now it refers to the policy of permitting employees to bring personally owned mobile devices (laptops, tablets, and smartphones) to their workplace, and to use them to access privileged company information and applications. Increased processing power and memory of smartphones and tablet computers have made affordable ability to use BYOD in educational process on a par with regular computer.

BYOD is in use at 59% of organizations with another 13% planning to allow it [2]. BYOD is most common in the manufacturing and education sectors, and there are more small companies, with 50 or fewer employees, allowing it when compared to larger organizations [2].

There are certain ways to organize access to a corporate or an educational network but nowadays most popular and affordable way appears IEEE 802.11 standards called Wi-Fi [3]. On the one hand it is convenient and easiest way to use your own mobile device in a classroom (or workspace), but on the other hand it brings more constrains for IT personal because of inherit technological drawbacks [4]. Most critical drawback is security issue. It is difficult to find balance between security and simplicity for users. Most algorithms were compromised recently. WPA and WPA2-PSK is no longer safe, with the appearance of high-speed brute forcers [5]. Moreover, the use of WEP and TKIP for confidentiality, authentication, or access control was deprecated and that algorithms are unsuitable for the purposes of standard 802.11 [6].

Analyzing challenges and variety of frameworks, it is obvious that BYOD security needs advance research and development. Scholars recommend implementing a multi layered approach when devising BYOD security policies [7][8][9].

This article devoted to practical results of implementing wireless access to educational network for students with BYOD in the SPO department of the ITMO University. This research has attempted to find a tradeoff between security and simplicity. It is two desirable but incompatible features that need to compromise.

II. Related work

BYOD was investigated and described in variety of papers [7][10][11]. Combining different frameworks and mitigating constraints could lead to unpredictable results. In order to paper of Kathlin Dower and Maumita Bhattacharya [7], implementing BYOD brings new challenges for IT department:

- Deployment challenge:
  - Determining how to implement BYOD security measures into existing networks.
  - Determining who in the organization need BYOD.

- Technical challenge:
  - Access control.
  - Providing ongoing support.
  - Maintaining secure and stable connection.
  - Protecting company data stored on cloud facility.
- Policy and regulation challenge:
  - Local government regulations and laws.
  - Ethical and privacy issues.
- Human Aspect Challenge:
  - Training and education users.
  - User reactions, emotions and compliance of BYOD policy.

Wireless network standard and security techniques used by the higher educational institutes were analyzed in paper of Ranjana Shukla, Samad S. Kolahi, Robert freeth and Avikash Kumar [3]. It shows that 64% of the survived educational institutes use highly secure protocol. They have shown that current price of the new technologies is holding back some institutions from staring installing in the future.

There are a lot of researches pertaining security in Wi-Fi networks in itself. Obsolete algorithms, such as TKIP and WEP are not considered safe by the standard [12]. WPA/WPA2 algorithms are no longer safe because of possibility Men-in-the-middle attacks and Rogue AP [13].

Cisco and Microsoft has own frameworks for secure and seamless implementation wireless networks. [14]

Survey has founded that WPA2-Enterprise with RADIUS server standard, mostly popular among educational institutions [3]. In order to the research, about 64% educational institutions are using WPA2-Enterprise.

Inside the WPA2-Enterprise framework, a user must authenticate to the authentication server (RADIUS) using a secure and reliable EAP method. Although many EAP methods there are only two the most commonly used EAP methods: EAP-TLS and PEAP-MSCHAPv2 [14].

A. EAP-TLS

EAP-TLS, defined in RFC 5216 and well supported among wireless vendors, is one of the challenging methods in consequence of the certificate requirements. It provides authentication through the exchange and verification of X.509 certificates. Therefore, installing the correct certificates on BYOD and the authentication server is essential. Every end-user and computer, including the authentication server must possess at least two certificates: a client certificate, signed by the certificate authority (CA) and a copy of the CA root certificate.

EAP-TLS is the most secure method since the client's certificate cannot be forged. A user should make a personal client certificate as proof of identity. Afterwards, the client's certificate should be signed by the CA that issued it. It requires personal contact between IT-support and user. Ultimately, the authentication server must have a copy of the root certificate for the CA that signed the user's certificate.

B. PEAP-MSCHAPv2

The inner authentication protocol is Microsoft's Challenge Handshake Authentication Protocol (MSCHAP), meaning it allows authentication to databases that support the MS-CHAPv2 format, including Microsoft NT and Microsoft Active Directory. Behind EAP-TLS, PEAP-MSCHAPv2 is the second most widely supported EAP standard in the world. There are client and server implementations of it from various vendors, including support in all recent releases from Microsoft, Apple Computer and Cisco.

PEAP-MSCHAPv2 authentication relies on a password, not certificate as EAP-TLS and traffic is encrypted using TLS. A CA certificate must be used at each client to authenticate the server before the client submits authentication credentials.

For secure connection every user that participates in PEAP-MSCHAPv2 must possess the following credentials: Root CA certificate for the CA that signed the certificate of the authentication server and MSCHAPv2 username and password.

If the CA certificate is not validated, in general it is trivial to introduce a fake Wireless Access Point, which then allows gathering of MSCHAPv2 handshakes [15].

III. IMPLEMENTATION

The SPO department constantly strives to improve strategies of IT management. It makes the best to provide access to the network for each student and at the same time always pursuits to minimize cost of supplying customers. There are certain challenges for the department through the framework provided by Kathlin Dower and Maumita Bhattacharya [7]:

A. Deployment challenge

Determining how to implement BYOD security measures into existing networks

To provide high level of security for an educational institution, wireless network for BYOD should be separated from backbone network. Access controlling, queuing, shaping and policing are very desirable. Under no circumstances BYOD should interrupt the backbone network's work.

Determining who in the organization need BYOD

It is important to provide access to the educational network to each member involving in an educational process. Largest group is students. 73.8% of the SPO department's students use BYOD for education each day. 36.1% have one BYOD and 50.8% carry 2 personal devices for educational purpose. Tutors (teachers) and other employees group are smaller but need to be prioritized higher. Using CIS is mandatory so employee need stable connection on a regular basis.

B. Technical challenge

Access control

Access control could be organized on a various level. First and most important level is Level-2, where 802.11x authentication take place. The survived network is using PEAP-MSCHAPv2 authentication. MAC control is used as

addition measure. Only a valid MAC addresses can enter the network.

Providing ongoing support

A current price of the new technologies is holding back some institutions from staring installing in the future [3]. Having specialists on a regular basis could be costly. The SPO department always strives to decrease expenses on IT-supplying by implementing high level of automatization.

Maintaining secure and stable connection

There are a lot of devices that have to work in an 802.1x networks but some of them inconsistent and behave unpredictably. Drivers sometimes make things worse. Some users have obsolete devices that have no support of this feature at all.

Protecting company data stored on cloud facility

This paper doesn't cover Layer 3 and upper lever security. Other protection techniques should be implemented to secure educational services inside network. Furthermore, most corporate cloud services are presented in the Internet, so have already had inherit security.

C. Policy and regulation challenge

Local government regulations and laws.

In order to the Russian Federation's law it is illegal to give someone unauthorized and anonymous access to a public network. Any network operator providing public access to a Wi-Fi network must collect user's personal data, such as name, surname or any ID. As long as there is no liability for this infringement a lot of organization still use open Wi-Fi without registration but it is not completely legal. So, Russian educational institutions are limited with using Wi-Fi without password and registration.

Ethical and privacy issues

The main issue with wireless security is the control on the communication medium. Open system can't get security for anyone but presents easiest and uncontrolled way of connection. EAP-TLS is the most secure and reliable for IT suppliers but difficult and undesirable for users. PEAP-MSCHAPv2 puts burden of security on users but more controllable and considered in this paper as tradeoff between easiness and security.

D. Human Aspect Challenge

Training and education users

The hardest part about implementing secure Wi-Fi appeared training the users. Users today have incredibly high expectations for ease of use. They also have more options than ever before to work around official access. If the network is too hard to use, they'll use data. If the certificate is bad, they will ignore it. If they can't access something they want, they will use a proxy.

User reactions, emotions and compliance of BYOD policy

This survey has assessed user's feedback. Measurements of overall level of our customer satisfaction found that easy access to the network is very important for students. Most student and employees tend to sacrifices security to the simplicity.

IV. RESULTS

In the 2013-2014 our students and employee had to apply for a PEAP-MSCHAPv2 login (or EAP-TLS certificate) personally. Dedicated specialist on a regular basis was responsible for registering new users, and consulting them. We had about 56 and 96 requests for a 2012-13 and 2013-15 year respectively (Figure 1).

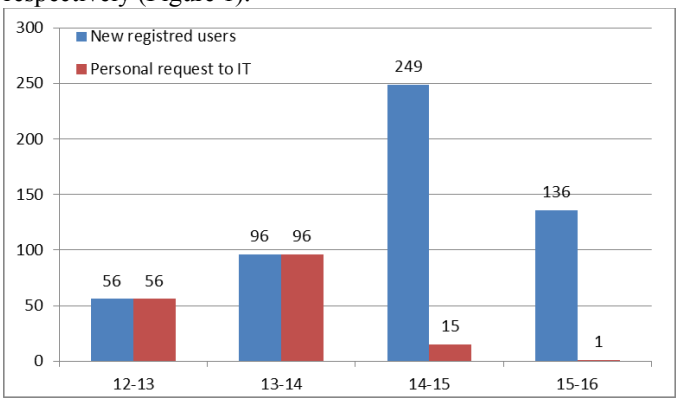

Fig. 1. Amount of new registered users per educational year

Measurements of overall customer satisfaction level found that easy access to the network is very important for students. In the 2014 the department implemented fully automated registration for students and employees through CIS (Corporate Information System) [15][12]. All students and employees registered and authenticated in the CIS is able get personal login PEAP-MSCHAPv2 in "one click". It caused increase of new users in the network, and, at the same time, it caused cutback of requests to the IT-support. In the 2015 we implemented some tutorial and advertising campaign and then discarded IT specialist relating to Wi-Fi on an every-day basis.

Total amount of student and employees in 2012-13, 2013-14, 2014-15 and 2015-16 is 532, 446, 480 and 509 persons each year respectively.

Easy access to registration and absence of every-day IT support resulted in slight increase of "never connected users", who got login but never managed to connect (Figure 2).

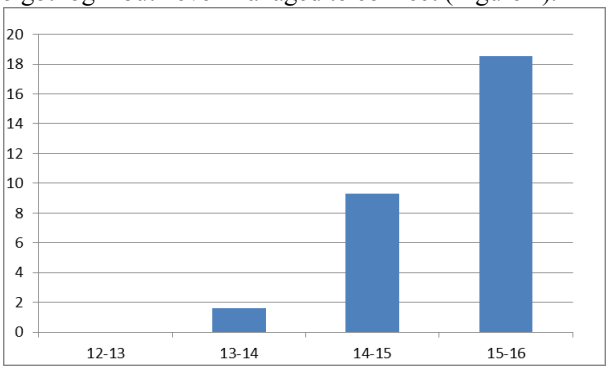

Fig. 2. Percent of registered but never used network users per year

The department asked students and employees to estimate importance of security and simplicity from 0 to 10. 0 – means no security at all (open Wi-Fi), 10 – means EAP-TLS and necessity installing certificates. 42% of the students and employees don't want to use any reliable security protocols and

consider it as disturbing. Only 17% are ready and will use certificate-based EAP-TLS instead of password-based PEAP-MSCHAPv2.

Finally, survey found that 43% of our students don't use CA certificates to authenticate the server during PEAP-MASCHPv2 based authentication. Consequently, "Rouge AP" and "Men-in-the-middle" attacks are the biggest threat against an educational wireless network. While WPA2 sets up a very secure connection, we also have to be sure that the users will only connect to the official network. A secure connection is meaningless if it's to a honeypot or imposter signal. Institutions often sweep for and detect rogue access points, including Man-in-the-Middle attacks, but users can still be vulnerable off-site. Even if the server has a certificate properly configured, there's no guarantee that users won't connect to a Rouge SSID and accept any certificates presented to them. Some operating systems make things worse: Android doesn't use CA certificate by default and more tend to compromise PEAP-MSCAHPv2 login and password connecting to Rogue AP. Windows, iOS and Macintosh show warning messages then certificate changes but users don't take it seriously most of the times. Android OS are very popular among students end employees (Table 1) and 26.24% may come across Rogue AP without warning messages.

TABLE I. USAGE OF OPERATING SYSTEM IN THE DEPATRMENT

Operating system	***Percent of users***
Windows	51,68%
Android	26,24%
iOS	12,10%
Macintosh	6,40%
Linux	1,89%
Windows Phone	1,65%
Unknown	0,02%
BlackBerry	0,01%

V. CONCLUSION

It is a vital to allow access for BYOD users to an educational network. Most educational institutions are using authentication. Security and simplicity are two desirable but incompatible features that need to compromise. But since security is burden of users they tend to use simple ways of connection compromising network even in case we make deal with experienced users. Therefore, level 2 cannot be the single level of security, but needs to be covered by security on upper levels.

REFERENCES

[1] V. Korolyov, D. Grinshpun, "The technology of surpassing studying in the system of continuous qualified education", IACEE World Conference on Continuing Engineering Education, WCCEE 2012.

[2] Teena Maddox, "BYOD, IoT and wearables thriving in the enterprise", 2016, [Online] Available: http://www.techproresearch.com/article/byod-iot-and-wearables-thriving-in-the-enterprise/

[3] Ranjana Shukla, Samad S. Kolahi, Robert freeth and Avikash Kumar, "Educational Institutes: Wireless Network Standards, Security and Future", Computer Sciences and Convergence Information Technology (ICCIT), 2010 5th International Conference.

[4] Amirali Sanatinia, Sashank Narain, Guevara Noubir, "Wireless Spreading of WiFi APs Infections using WPS Flaws: an Epidemiological and Experimental Study", 6th Symposium on Security Analytics and Automation 2013

[5] Lui Yong-lei, "Defense of WPA/WPA2-PSK Brute Forcer", 2015, 2nd international Conference on Information Science and Control Engineering.

[6] IEEE 802.11-2012 Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specification (2012)

[7] Kathleen Downer, Maumita Bhattacharya, "BYOD Security: A New Business Challenge", 2015 IEEE International Conference on Smart City/SocialCom/

[8] Simon Denman, "Why multi-layered security is still the best defence", Network Security, Vol 2012. Issue 3.Pp. 5-7

[9] Rhodes J (2013), "Building Security Around BYOD. Managing Mobility, Rough Notes". Vol 156. Pp 104,114.

[10] V. Shakhalov, L. Zinchenko, E. Rezchikova, A. Glushko, An Opportunity in Engineering Education Russian BYOD Tendencies, 2015 International Conference on Interactive Collaborative Learning (ICL).

[11] Sara Ali, Muhammad Nauman Qureshi, Abdul Ghafoor Abbasi, "Analysis of BYOD Security Frameworks", 2015 Conference on Information Assurance and Cyber Security (CIACS)

[12] V.Korolyov, D. Grinshpun, R. Nuretdinov, "Change management in continuing engineering education in IT (on the example of secondary vocational education faculty of ITMO University)", 15th world conference of international association of continuing engineering education, IACEE 2016.

[13] N. Asokan, Valtteri Niemi, Kaisa Nyberg, "Man-in-the-Middle in Tunneled Authentication Protocols" Nokia Research Center, 2002.

[14] Cisco, "Wired 802.1X Deployment Guide", [Online] Available http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Security/TrustSec_1-99/Dot1X_Deployment/Dot1x_Dep_Guide.html

[15] A. Lukin, R. Nuretdinov, D. Grinspun, "Electronic system of controlling educational process with elements of results predictions", Sociosphere: Modern technologies in system of additional and professional education, 2014.