Lightweight approach for WiFi network access and monitoring

Marcin Bajer[1]

ABB Corporate Research Krakow, Starowilna 13A, Krakow, Poland,
marcin.bajer@pl.abb.com

Abstract. The goal of this publication is to describe lightweight, cost effective approach for creating access and monitoring system for WiFi network in small and medium size buildings.
The basic assumption is that the system should support per user authentication and provide network health and usage statistics.
In contrast to current market available solutions the presented one requires very little modification of off-the-shelf SOHO type routers to enable wide range of new functionalities. The core or the system is based on OpenWRT Linux running on multiple WiFi access points spread throughout the building. For data storage and visualization centralized solution prepared based on Node.js server and AngularJS front-end and running on Raspberry Pi 2 development board is used.

Keywords: netowork monitoring, access control, RaspberryPi, node.js, smart home

1 Introduction

It is expected that the WiFi market will continue to grow tremendously over the next few years. One of main driving factors for this is the increasing number of smart devices (mobiles phones, tablets, smartwatches and smart TVs. . .). The observed pattern is to maximum data usage by the end users when they are stationary connected to WiFi in homes, offices or public buildings. Additionally, even though the falling prices of mobile transfer, it is common that smart devices are configured to trigger data intensive applications such as updates and synchronization only while being connected to WiFi.

For many years the focus in network security was placed on protecting network from external threats using firewalls and public key cryptography. Nowadays, attention has turned towards protecting crucial network resources against the ”enemy within”. Small businesses are often in a difficult position when it comes to network security. On one hand the growing demand for WiFi access is pushing them towards allowing more users to access their WiFi network, on the other hand they lack the cheap and secure solution for doing so. The main requirement for them is to enable secure per user access and monitoring.

In addition, nowadays, network devices are not limited to not regular laptop/smartphone devices. It is expected that number of IoT devices will far exceed that of other connected devices [1]. Very often it is expected that those devices are separated for regular network and additional security level is implemented. For case of some IoT applications it is also crucial to ensure sufficient level of network reliability.

Separate topic is WiFi piggybacking. Apart from security issue, unauthorized access to network can result in steeling bandwidth, but what is far worse, piggybacking can be used also as a means of hiding illegal activities (pornography, torrenting. . . etc.) impersonating authorized network user. Such illegal activities can be also performed by authenticated users, in this case it is important to be able to trace web activity to the particular user of the network, otherwise network owner would be prosecuted.

Further in this paper, the approach for preparation of internal WiFi network in medium size rent house is presented. The goal of the project is not only to provide WiFi network to the users, but also to setup backbone for planned smart home installation.

Of course, monitoring and access control is only a part of complex topic of network security. Apart from controlling how the network is used, it is necessary to protect the network from attacks that are aim to disclosure or corrupt sensitive data as well as influence on proper work of network elements. Those problems will not be addressed in this paper since in case of described installation it was decided that additional protection against such actions is not needed.

2 Network requirements

The goal of this project was to prepare internal network in tenement house. The assumption for network to be prepared was to provide:

1. Fast and reliable WiFi throughout whole building,
2. Cost-oriented implementation,
3. Separate isolated virtual subnetwork for critical devices, such as surveillance cameras, smart home automation devices or network attached storage,
4. Easy to manage, per user, Internet access for guest devices via dedicated subnetwork,
5. Web page for network administration accessible both internally and externally,
6. External access to internal network via VPN tunnel.
7. Backbone for planned smart home installation.

In the subsequent parts of the paper, each of this requirements will be addressed.

3 Fast and reliable WiFi throughout whole building & cost-oriented implementation

Modern enterprise class WLAN solutions are feature-packed, complicated and, what is the most important, quite expensive. For customers on tight budgets, there are a lot of low-cost WiFi devices which can be fitted with open-source software to provide business-class WiFi features. This would require some additional work and trade-offs, but can result with interesting feature sets that typically are beyond reach for small budgets.

This paper will describe implementation of WiFi network with one router and 6 access points. It was decided to use one hardware for all of the devices. After cost-capability assessment it was decided to use TpLink WRT4300 SOHO type router. It offers Gigabit Ethernet and concurrent dual band wireless N750 transfer. It can support 300Mbps on the 2.4 GHz (dual-stream 2x2) and 450 Mbps on the 5 GHz Band (triple-stream 3x3). The hardware platform is based on Atheros AR9344@560MHz and 128MB RAM. In addition, the device was equipped with 800Mbps hardware NAT and 2 USB v2.0 ports.

The factory firmware was replaced by custom compiled OpenWRT Barrier Breaker build. Configuration details and build instructions can be find in [2]. The firmware is the same for all devices and contains all required packages compiled into SquashFS ROM partition. The difference is only in configuration, so in case of malfunction it is possible to easy replace broken device. For future use, it is also possible to download needed packet from OpenWRT packet repository and place it into JFFS2 data partition.

On each floor of the building two APs were located. Each provides WiFi coveradge and wire LAN connections for this segment of the building. In the future, USB ports in APs will also be used for connectivity with elements of smart home automation devices (automatic meter reading, light control. . . etc.). Original power adapters for the routers has been replaced with one central power supply on each of the floors.

4 Separate isolated virtual subnetwork for critical devices

The separation of the devices is done using VLAN mechanism. Two VLANs were configured in the building. First, isolated guest network for tenants, which allows only Internet access. Second, administration network, for building infrastructure and administration (IP cameras, IoT devices, VoIP intercoms). To implement this idea, in each of APs, four WiFi networks were created (two for 2,4GHz and two for 5GHz band). Only two network SSIDs were used, one for the guest network and second for administration network - this allows that the user is automatically routed to the AP which provides the best signal. The WiFi networks are linked to the VLANs in the way both 2,4GHz and 5GHz band provides access to both VLANs. Ports of the AP switch which are connected to the network backbone use VLAN tagging to distinguish traffic associated with different VLANs. In this way AP is connected only with the one cable (so called trunk link) to the router/other switch. Each VLAN is also a separated subnet. Router only allows to forward traffic from administration network to the guest network.

5 Easy to manage, per user network access

5.1 Choosing an WiFi encryption method

It is known that Wired Equivalent Privacy (WAP) based approach for securing WiFi network contains serious vulnerabilities that allows to easily crack password protecting the wireless by sniffing airwaves [3]. Therefore, it is highly recommended to use more secure Wi-Fi Protected Access (WPA or WPA2) encryption method. WPA has two versions: PSK (Pre-shared key) and Enterprise. PSK version had also some vulnerabilities [4] which were adressed with introduction of AES-based encryption in WPA2. Generally, using WPA2-PSK AES together with complex, non-dictionary pass-phrase is considered as safe solution, but it has significant drawback of using common key across all users. In case password is compromised all devices in the network reprogrammed. Solution to this problem is to use WPA/WPA2 Enterprise. In contrast to WPA-PSK each has given unique credentials (user/password or digital certificate). Traditionally, the WPA-Enterprise implementation requires purchasing dedicated server device. To reduce costs, further in this paper process of installing FreeRadius server on Raspberry Pi 2 device will be described.

5.2 Authentication, authorization, accounting

An Authentication Authorization Accounting (AAA) [6][7] is a security architecture model. It was designed to authenticate and authorize users for use of network resources. Authentication part confirms that a user who is requesting a service is a valid user. Authorization grants specific types of service to a user, based on their authentication. Accounting refers to the tracking of the consumption of network resources by users.

5.3 Extensible Authentication Protocol

To replace proprietary solutions and provide unified authentication framework EAP (Extensible Authentication Protocol) was specified [5]. EAP provides framework for several different authentication methods (MD5, TLS, TTLS, LEAP, PEAP). The authentication method used to verify the user (and server) credentials on WPA/WPA2-Enterprise networks is defined in the IEEE 802.1X standard which is simply a standard for passing EAP over a wired or wireless LAN (EAPoL - EAP over LAN). Complete IEEE 802.1X system is composed of three-component architecture: supplicant (end user station), access device (switch, access point) and authentication server (RADIUS). EAPoL communication occurs between supplicant and authenticator. The RADIUS protocol is used for communication between the authenticator and the RADIUS server. In presented installation the authenticators are OpenWRT APs. To provide possibility to authenticate users with Radius server *wpad-mini* packet (default WPA implementation for OpenWRT) has been replaced with *wpad*. The easiest way to configure authenticator is to use LuCI (web administration interface of OpenWRT). Beside standard configuration of WiFi AP (ssid, encryption type. . . etc.), it is required to configure IP and port of Radius server together with a secret key to authorize AP to the server.

Router and other APs are considered as clients for Radius server configuration.

5.4 Radius server

Remote Authentication Dial-In User Service (RADIUS) [8] is the most widely used protocol to provide AAA. For the network presented in this publication FreeRadius [9] has been chosen. This modular, feature-rich, open source implementation of RADIUS protocol is one of the most commonly used. Radius server is available as OpenWRT packet and can be easily installed. Configuration of FreeRadius can be a complex task, but in most of cases default configuration is the best one. It is beyond scope of this paper to describe details of FreeRadius configuration. For details refer to configuration files stored in [2].

Although, tests shown that also Radius server can work on TpLink WRT4300 based APs without noticeable performance impact, it was decided that it will be moved to Raspberry Pi. Since all needed packets are compiled into AP's firmware, in case of Raspberry Pi breakdown, it is easy to start Radius server on any of them (just activate Radius server process, configuration has been deployed during commissioning).

5.5 AAA implementation summary

WPA2 Enterprise has been used only for the WiFi guest network. Administration network is protected via regular WPA2 PSK. Unfortunately, not all embedded devices support enterprise-grade wireless security (i.e. IP cameras).

It was observed that WPA2 Enterprise has one significant drawback in case of Windows based devices - configuration of the connection is a bit complex.

To reduce load on router, the server is running on one of the WiFi access points.

EAP provides framework for several different authentication methods. General idea is that it supposed with standarized approach to whole authentification process. There are many different EAP implementations , WPA, WPA2. . . etc.).

(password exchange, challenge-response tokens and public-key infrastructure certificates all work smoothly.

response tokens and public-key infrastructure.

standarised authentication mechanism

EAP is supposed to head off proprietary authentication systems and let everything from passwords to challenge-response tokens and public-key infrastructure certificates all work smoothly.

In described network it was decided that two VLANs were created. First one is publicly available and protected with EAP. It is used by "guests" in the building (renters, visitors. . .) who login with their unique credentials. Second VLAN

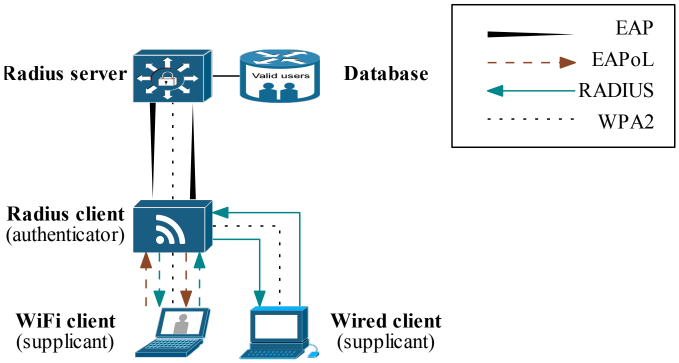

Fig. 1. Complete IEEE 802.1X system.

is dedicated for building administration (network storage, cameras, smart home automation devices. . .) and popentially can be used for non EAP compliant devices. Security of this crucial building equipment is ensured both physical separation (key protected cabinets, straitened access) as well as logical (non-trivial WPA2-PSK WiFi password, firewall filtering access from outside the network, MAC based IP lease by DHCP).

Hostile traffic

and guests in a building and flat renters,

and a separate one, available only in key protected cabinets dedicated for non EAP compliant devices (i.e. cameras). Security of crucial network equipment (i.e. smart home automation, network strorage devices)

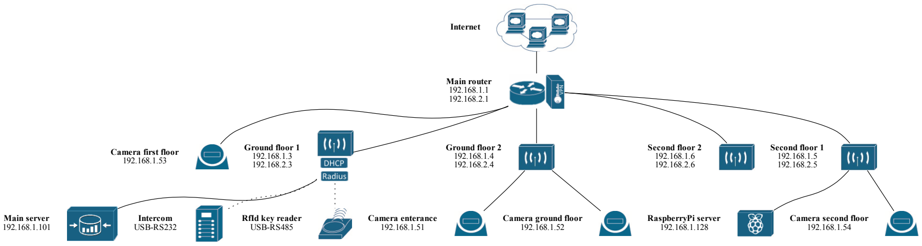

Fig. 2. Topology of prepared network

References

1. Middleton, P., Kjeldsen P., Tully J., Forecast: The Internet of Things, Worldwide, Gartner Inc., November 2013

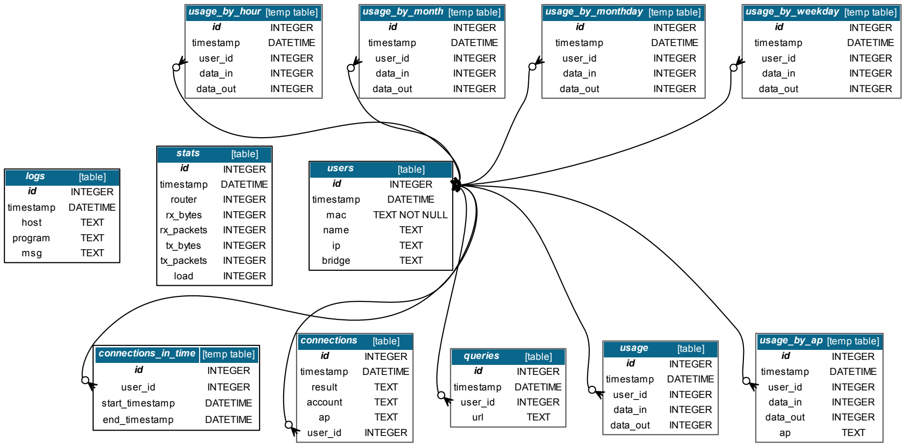

Fig. 3. Schema of database

2. Bajer, M., GitHub repository of SmartBuilding project, `https://github.com/bajerwitharm/smartbuilding`,
3. Ossmann, M., WEP: Dead Again Part. 1, Security Focus, `http://www.bandwidthco.com/sf_whitepapers/wireless/WEP%20-%20Dead%20Again%20Part%201.pdf` (accessed 2014.12.10),
4. Moskowitz, R., Fleishman, G., Weakness in Passphrase Choice in WPA Interface, WNN Wi-Fi Net News, `http://wifinetnews.com/archives/002452.html` (accessed 2014.12.10),
5. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.E., Extensible Authentication Protocol (EAP), RFC 3748, June 2004, `http://tools.ietf.org/html/rfc3748`,
6. de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., and D. Spence, Generic AAA Architecture, RFC 2903, August 2000, `http://www.rfc-editor.org/info/rfc2903`,
7. Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, AAA Authorization Framework, RFC 2904, August 2000, `http://www.rfc-editor.org/info/rfc2904`,
8. Rigney, C., Willens, S., Rubens, A., and W. Simpson, Remote Authentication Dial In User Service (RADIUS), RFC 2865, June 2000, `http://www.rfc-editor.org/info/rfc2865`,
9. FreeRadius technical guide, `http://networkradius.com/doc/FreeRADIUS%20Technical%20Guide.pdf` (accessed 2014.11.29)