Problems security solution by data transmission in ubiquitous systems based in Rijndael´s algorithm to Wi-fi routers

Salvador Gómez Pedraz[1], Juan Antonio Rodrigo Yanes[2], José Antonio Gutiérrez de Mesa[3], Javier de Pedro Carracedo[2]

[1] Universidad Rey Juan Carlos, Dto. de Informática
28903 Leganés, Spain
sgpedraz@inf.uc3m
[2] Universidad de Alcalá, Dto. de Automática,
28001 Alcalá de Henares, Spain
jrodrigo@aut.uah.es
{Bernauer, Wiese}@Springer.de
[3] Universidad de Alcalá, Dto. de Ciencias de la Computación,
28001 Alcalá de Henares, Spain
jagutierrez@uah.es

1 Introduction

At present one of the most important factors that define the managerial evolution is the connectivity give by means of electronic mechanisms, mechanisms that are not exempt from assaults that determine the integrity of the information that is transmitted or the confidentiality of the same one. In our society the availability of the information is given priority as preponderant factor in real time, therefore it is not only important to have access to the information, but to have access to the correct information of rapid and sure form.

These aspects related to the information and to the sure communication of the same one, make that most of the companies has a direct dependence of the means that allow to interchange information of dynamical form with any part of the world, without delays and with the safety of which the interchanged information answers to the beginning of the computer safety: Integrity, Confidentiality, Availability and Don't-repudiates, as well as the Accessibility.

The safety of the wired up nets is by itself complex enough of managing knowing the spatial limits of our systems. With the wireless nets an extra is going to be added to the above mentioned complexity having to be protected from two important points of view:

- The sensitive information in traffic of the users of our system that they choose for the connections Wireless (Privacy and Confidentiality) and
- The protection against the attackers' intrusion inside our net (Authentication of connections).

To the nets Wireless it is necessary to apply all the possibilities of assault that take are produced in the nets wired up, plus all the possibilities of the nets broadcast and the intrusion of preachers in our systems.

In the present article one tries to reach port a contribution in the area of safety in the wireless communications to solve the aspects of weakness detected in this field, and that do not allow to guarantee to the users of the same one a few minimums in the aspects of confidentiality and integrity in the sent or received information.

Across an exhaustive bibliographical review one makes the existing weaknesses clear in the definite protocols of authentication and coding in the standard on 802.11, as well as the assaults that can be realized and the tools that are in use for simplifying the process. Once demonstrated these deficiencies, there is realized a detailed study of the possible solutions, proposing the one that is considered to be more adapted from the technical point of view: the algorithm of coding AES (Rijndael's algorithm). This solution is implemented in a wireless standard platform to realize the process of validation across experimental confirmed tests.

Once analyzed and confirmed the experimental obtained information, it gives like proved the offer of the AES as algorithm of coding and of authentication to obtain a safety level more adapted to the levels of implantation of the wireless nets as to domestic as managerial level.

2 Security problem

Due to the characteristics of the safety mechanisms of the wireless nets that answer to the standard 802.11, it is evident that because of the specificities of the used protocol, the RC4, the deficiencies that already existed for the same one, and the mistakes of implementation of the same one, we would going to discover vulnerabilities that were concerning the reliability of these mechanisms of safety. These vulnerabilities remained clear in a time reduced, like it appears in the following scheme:

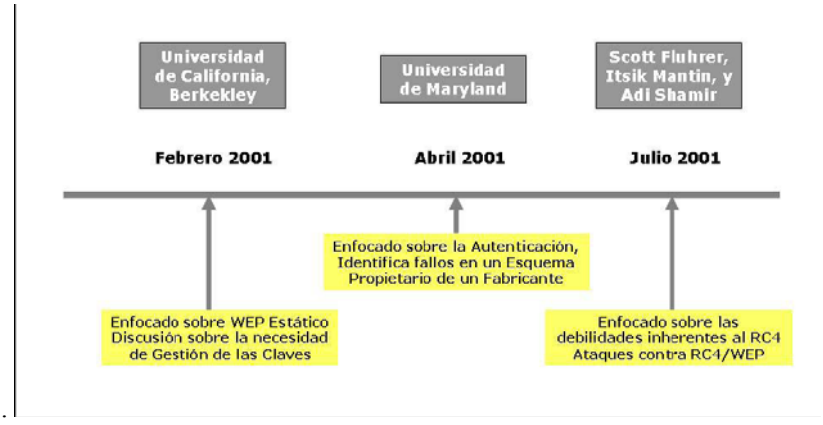

Fig. 1. Scheme of identification of vulnerabilities WEP in chronological order.

In the first reference, we take as base the protocol WEP (Wired Equivalent Privacy) as component of the standard 802.11 of the wireless nets, bearing in mind that is the base to protect the assaults to level scales of link. Borisov, Goldberg and Wag-

ner, of Berkeley's University [1] discovered several serious failures in the safety of this protocol, came from the bad utilization of the original ones of coding. Failures give place to a number of practical assaults that demonstrate that the failures of the WEP prevent from obtaining their goals. In the mentioned article, there are discussed in detail each of the failures, the principal violations of safety and the assaults to which they give place.

The second reference to put in manifest the vulnerability of the WEP, consequently of the safety of the standard 802.11, was elaborated by Arbaugh, Shankar and Wan, from the University of Maryland [2]. In that article they allude to problems of safety in the points of access of the wireless nets. It maintains that users and organizations think that the safety facilitated by the above mentioned points of access is sufficient, which increases in major measurement the risk of the above mentioned nets. This makes nets specially vulnerable to fraudulent uses of the same ones.

Finally, in the last milestone to put of manifest the safety shortage of the WEP, Fluhre, Mantin and Shamir [3], did a complete study on the weaknesses that presents the algorithm of planning of keys of the RC4 and the way to carry it out, on that there is based the protocol WEP. In this article, they check the weaknesses based on key weak persons and on the characteristics of implementation of the RC4 in the relating thing to the utilization of the Vector of Initialization the (IV)th and of the keys to code different messages.

To the commented in the previous paragraphs it is necessary to add the principal problem of the wireless nets: " the fault of precautions of the owners ". In a great number of cases the wireless nets that the users install, especially domestic users or small enterprises, leave the configuration for fault: Broadcast SSID, Open System authentication, without coding WEP and no filtering directions admitted MAC.

With all these preambles, the difficulties to get in a wireless net are minimal, especially if to all that we add that in many nets there is activated a servant of dynamical ip addresses DHCP.

2.1 New security protocols

After the reading of the previous articles it is confirmed that the safety is one of the weakest points in the standard 802.11 in any of the versions that we could use. All this, even being a patent for yes same, it becomes more worrying by the great summit that is taking this type of nets so much to managerial as domestic level. Though they do not form a part of the standard, the manufacturers of devices Wi-Fi, they decided to offer the possibilities of using keys of double length (from 64 to 128 bits). WEP used with keys of 128 bits is WEP2. Nevertheless, we must observe that the length of the vector of activation continues being of 24 bits (the plots IEEE 802.11 do not contemplate a major number of bits to send the IVth), for what the only thing that there is secret key (of 40 bits to 104 bits). Due to the fact that the length of the IVth and the way of using it do not change, the weaknesses of the IVth can continue being taken advantage of the same way for what it is possible to affirm that WEP2 does not solve WEP's problems [4].

Another WEP's variant used in some implementations is *dynamical WEP*. In this case one seeks to incorporate mechanisms of automatic distribution of keys and of authentication of users by 802.1x/EAP/RADIUS. A servant needs of authentication (RADIUS normally) working in the net. In case the key (key secretes + WEP) is not in use in any more than one plot it would be sufficient to compensate WEP's principal weaknesses. Nevertheless, the solution preferred by the companies has been VPNs's utilization, in the same way as it would be done if the users were connected remotely to the office. VPNs's technology is sufficiently proven and is considered to be sure though it has not been designed specifically to be used in nets of ubiquitous computers. It haves the disadvantage of interoperability between devices of different manufacturers.

Once assumed the problem, the members of the group of work of the IEEE take the determination to elaborate a new standard that completes and corrects the deficit in safety topics that had been detected up to the moment. The mechanisms designed specifically for nets WLAN to be the successors of WEP are WPA [5] and WPA2 [6].

In an analysis of the standard WPA realized by Glenn Fleishman and Robert Mosko-witz [7] and Moen, Raddum and Hole [8] the safety level of the same questions, indicating that in certain circumstances can offer less safety than the current systems like WEP, which have been demonstrated like slightly sure.

2.2 New Standard of advanced cipher (AES)

In 1996, National Institute of Standards and Technology (NIST) gave the first steps for the consolidation of a Standard of Advanced Coding (Advanced Encryption Standard, AES) [9]. The general aim of this one summons were to develop a specification to find an algorithm of coding that replaces the dying person DES (56 bits of key, why it turns out to be insecure nowadays, and design orientated to hardware, why it turns out to be relatively inefficient in software), so that the new algorithm is capable of protecting the sensitive information of the citizens and of the government up to good entered the XXIst century. It was hoping that the selected algorithm was used by the Government of The United States and of voluntary form by the rest of sectors involved in safety topics, including the private sector, in DES's substitution. For extension it would be used by the countries of the rest of the world.

In January, 1997 [10], and across the Department of Trade and the NIST by means of the document " Announcing Development of to Federal Information Processing Standard for Advanced Encryption Standard " carried out a summons for the presentation of algorithms, in which there were specified diverse criteria of evaluation and minimal requirements of acceptance.

Come to this point the NIST had to take a decision of commitment between safety and efficiency, both in the development and in the execution or the costs of accomplishment of the same ones in hardware. Due to all these ends the election of an algorithm of coding is really difficult because it will depend directly on the platform in the one that is going to be executed, the language of programming in the one that is

going to develop and the future development that is going to have, especially if it is going to develop in hardware [11].

The conclusions to those who can come near are to which the NIST came, and they were that, when there is done a study of all the factors in its set, safety analysis, details of implementation, yield and capacity for integration in hardware, "Rijndael is a safety combination, yield, efficiency, capacity of interoperability and flexibility that makes that he is the candidate adapted for its selection as AES". The algorithm Rijndael was chosen principally for guaranteeing safety, which means to be immune to the known assaults, to have a simple design, and to be able to be implemented in the majority of the possible scenes, from devices with limited resources, from smart cards to parallel processors. The time has allowed that AES should be adapted little by little, from the protocols most used as SSL, up to the applications more specialized, as in VoIP [12].

3 Implantation of the algorithm

3.1 Aim

Once come to this, one worked in implementing this algorithm in some rou-ter commercial WiFi in order to evaluate its performance for it diverse scenes were selected in order to decide the basic platform to using that, after several studies, decided, fundamentally for the evaluation of diverse platforms on those who can be loaded firmware alternative based on Linux and OpenGL (LinuxAP), to choose Access/Router of Linksys's Point, the WRT54G, which principal characteristic is that it haves integrated by fault a system minimal Linux. The manufacturer includes, besides this minimal system, the corresponding functions for the correct functioning of the AP/Router after a time of opaqueness that was breaking with the commitments of the GNU GPL.

This selected platform possesses the additional advantage of having different alternatives in the shape of firmware free, based on the majority of the cases in the official firmware. This allows doing evaluations with different profiles of load of the system, since each of them has a configuration of the operative system, from minimal systems, which interfaces do not contemplate web, to complete systems.

3.2 Used Firmware: Alchemy Public Firmware

The firmware used for the design and evaluation of the code that allows a safety level adapted to the needs exposed in the aims of the present work, is the one that allows a major facility than the official firmware, but which is based on it, this characteristic

treats itself about a code source with more opened characteristics than the own code Linksys's source. This firmware at present supports as operative system Linux's nucleus 2.4.20 on which there have developed the functions of AES's implementation in order to measure its yield.

4 Efficiency test

Once introduced the system of functions in order that the router supports AES cipher and verified its correct functioning tried to study its yield in commercial conditions of utilization, for it an environment of validation was defined isolated regarding interferences of radio frequencies of other wireless nets that could operate on the same channel or the interferences of other channels, since they can be 1, 6 and 11.

For the accomplishment of the evaluation a location has been selected with no type of wireless nets. To find an immune location to the interferences in the spectrum of frequencies of the net tools are in use of scanned of frequencies and sniffer that will allow to identify if some net exists in the environment and, if so, the channel used by this net.

Due to what is claimed is to analyze the yield depending on the algorithm of coding; an analysis is in use with the systems placed in distances that do not influence the global yield of the system. The distances to which the tests are realized will not be superior to 10 meters.

The principal aim of the accomplishment of the measurements is to obtain a few information that allow us to value the suitability of the algorithm selected to take to end the coding they must obtain information perfectly repeatable in the selected scenes, and a selection of scenes with a fan that allows to valid the results for transmissions of different from systems of information. Of the same form it is necessary to have a few values of reference that allow us to confirm the influence, as of the transmission of wireless net as the influence of the algorithms of coding. Because of that there are realized ten measurements of files of different size to obtain a repeatable in the test, discarding the ones that do not adjust to the ranges of diversions established for the obtaining of the average values and of speed. The values of the selected sizes were 5 Mb, 10 Mb, 15 Mb, 20 Mb, 30 Mb, 50 Mb, 75 Mb, 100 Mb, 125 Mb and 150 Mb, respectively, and the obtained ones were in use as values of reference and contrast with wired up net Ethernet 100 Mbps, whose values were obtained of the same computers, the same application and scene of reference and that show themselves in the table 1

SRV-PC Cable Cruzado				
	Tamaño del fichero (Mbps)	Tiempo (s)	desviación	Velocidad (Mbps)
Fichero 1	5	2,388	0,0527	2,094
Fichero 2	10	4,754	0,1931	2,104
Fichero 3	15	6,963	0,0683	2,154
Fichero 4	20	9,288	0,1582	2,153
Fichero 5	25	12,171	1,1382	2,054
Fichero 6	50	23,978	0,3856	2,085
Fichero 7	75	34,844	0,1195	2,152
Fichero 8	100	48,468	1,4724	2,063
Fichero 9	125	58,291	0,9517	2,144
Fichero 10	150	69,505	2,0075	2,158
Velocidad Media				**2,116**
Desviación Velocidad				**0,0408**

Table 1. Values of reference with wired up Ethernet 100Mb.

4.1. Resultados medidos

Because of the characteristics of the system that is going to be evaluated, it is considered suitable to have the information of reference of a wireless standard net, with the original devices (without modifications) as in hardware as in firmware. The scene that is going to be had of reference is the one that appears in the following figure:

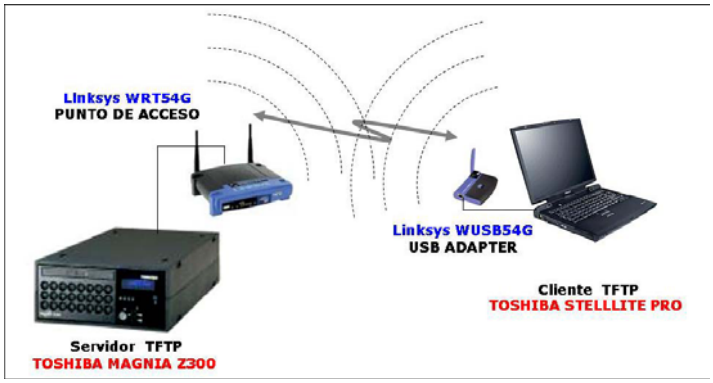

Fig. 2. Escenario 1.- Server -AP-Client with USB card.

In this scene it is possible to observe that the red is integrated by a point of access by the same platform hardware that the selected to realize the work, but with Linksys's original, as it comes from factory. The connection between the servant and the point of access is realized by net Ethernet and cable RJ45 CAT6.

In another end, in the computer that acts as client, we install a wireless net adapter USB of 54 Mb. Variables are taken by the following configurations: without coding, with coding WEP of 64 bits and with coding WEP of 128 bits (at the moment there are not tested coding AES because we don't dispose it in the configurations of the manufacturer).

With these configurations the following results were obtained

SRV-BRIDGE-PC				
CLAVE:NO		LONGITUD: -		
	Tamaño del fichero (Mbps)	Tiempo (s)	desviación	Velocidad (Mbps)
Fichero 1	5	3,892	0,2834	1,285
Fichero 2	10	7,571	1,0021	1,321
Fichero 3	15	11,092	0,9284	1,352
Fichero 4	20	15,353	1,0324	1,303
Fichero 5	25	19,236	0,4917	1,300
Fichero 6	50	38,356	0,0456	1,304
Fichero 7	75	57,557	0,6143	1,303
Fichero 8	100	77,421	1,5629	1,292
Fichero 9	125	96,123	1,8945	1,300
Fichero 10	150	116,207	0,9308	1,291
Velocidad Media				**1,305**
Desviación Velocidad				**0,0193**

:

Table 2. Results with WEP coding of 64 bits.

SRV-BRIDGE-PC				
CLAVE:WEP		LONGITUD: 64		
	Tamaño del fichero (Mbps)	Tiempo (s)	desviación	Velocidad (Mbps)
Fichero 1	5	3,874	0,1020	1,291
Fichero 2	10	7,540	0,9545	1,326
Fichero 3	15	11,037	0,4315	1,359
Fichero 4	20	15,280	0,1148	1,309
Fichero 5	25	19,145	0,3043	1,306
Fichero 6	50	38,595	0,3856	1,296
Fichero 7	75	57,284	0,1195	1,309
Fichero 8	100	76,149	1,4724	1,313
Fichero 9	125	95,668	0,9517	1,307
Fichero 10	150	115,686	1,0200	1,297
Velocidad Media				**1,311**
Desviación Velocidad				**0,0196**

Tabla 3. Results with WEP coding of 128 bits.

Finally we make the measurements with the coding AES got in the basic configuration of the router and the following results are obtained:

SRV-BRIDGE-PC				
CLAVE:AES		LONGITUD: -		
	Tamaño del fichero (Mbps)	Tiempo (s)	desviación	Velocidad (Mbps)
Fichero 1	5	4,117	0,4152	1,214
Fichero 2	10	7,792	0,5761	1,283
Fichero 3	15	11,614	0,7855	1,292
Fichero 4	20	17,209	1,1966	1,162
Fichero 5	25	20,106	1,0664	1,243
Fichero 6	50	39,557	0,9990	1,264
Fichero 7	75	60,239	1,3437	1,245
Fichero 8	100	80,806	1,2729	1,238
Fichero 9	125	101,330	0,5705	1,234
Fichero 10	150	125,390	1,4452	1,196
Velocidad Media				**1,237**
Desviación Velocidad				**0,0391**

Table 4. Results with coding AES of 128 bits

.

If we do a comparative analysis among the different configurations of this scene, it is possible to observe that a considerable decrease exists opposite to the configuration of crossed cable. Likewise a decrease exists in the yield and the rate of transference opposite to the scene in which the client connects directly to the point of access by means of an adapter of net..

Also it is possible to observe that it doesn't exist a considerable decrease of speed motivated by the incorporation of the coding WEP, in any of its lengths. Introducing the coding AES of 128 bits, a decrease is detected in the yield of the system, but not obvious, already this decrease does not reach 10 %, information that can be confirm in the comparative summary showed in the table 5.

SERVER+AP-CLIENTES-PC		
	Velocidad (Mbps)	desviación
SIN CIFRADO	1,189	0,6317
WEP 64	1,149	0,0408
WEP128	1,074	0,0345
AES	0,996	0,0366

Table 5. Proved comparative

5 Conclusions

Once checked in the previous paragraph the contributions consequence of the accomplishment of the present article, the following conclusions can be emphasized:

- The safety contributed by the protocols proposed by the standard 802.11: WEP and WPA, are easily vulnerable, being perfectly documented these vulnerabilities, as well as the methods and tools that allow achieve these vulnerabilities in relatively short times and with an operative minimal complexity.
- To propose as alternative of algorithm of coding the AES (algorithm Rijendael). The implementation of the system proposes with a programming in language "C", based on offers optimized to improve it's yield.

The tests (proofs) of validation realized for this platform with the integration of the algorithm AES allow to state that the penalty that is obtained by the application of the new system; they are perfectly bearable to obtain speeds of transference of 54 Mbits.

References

1. N. Borisov, I. Goldberg, y D. Wagner, "Intercepting Mobile Communications: The Insecurity of 802.11.", (Jan 2001). http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.
2. W. Arbaugh, N. Shankar, y Y. Wan. "Your 802.11 wireless network has no clothes", (March 2001). http://www.cs.umd.edu/~waa/wireless.pdf .
3. S. Fluhrer, I. Mantin, y A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", (august 2001). http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf .
4. N. Borisov, I. Goldberg, and D. Wagner. "Intercepting mobile communications: the insecurity of 802.11". MOBICOM, (july 2001).
5. S. Fluhrer, I. Mantin, y A. Shamir, "Weaknesses in the Key Scheduling Algorithm of RC4", (agosto 2001). http://www.eyetap.org/~rguerra/toronto2001/rc4_ksaproc.pdf.
6. IEEE Std. 802.11i/D3.0. "Part 11: Wireless Medium Access Control (MAC) and physical layer control (PHY) specifications: Specification for Enhenced Security". (November 2002).
7. G. Fleishman, R. Moskowitz "Weakness in Passphrase Choice in WPA Interface", 2003.
8. V. Moen, H. Raddum, and K. J. Hole "Weaknesses in the Temporal Key Hash of WPA", (april, 2004) .
9. National Institute of Standards and Technology, "Announcing Development of a Federal Information Standard for Advanced Encryption Standard," Federal Register, v. 62, n. 1, 2 (Jan 1997), pp. 93-94.
10. National Institute of Standards and Technology, "Announcing Request for Candidate Algorithm Nominations for the Advanced Encryption Standard (AES)," Federal Register, v. 62, n. 117, (Sep 1997), pp. 48051-48058.
11. B. Schneier, D. Whiting, "A Performance Comparison of the Five AES Finalists", Counterpane Internet Security, Inc., Abri12000.
12. http://csrc.nist.gov/CryptoToolkit/aes/round2/conf3/aes3papers.html (febraury 2006)