ISSN: 0123-3033 – ISSN-e: 2027-8284

INGENIERIA Y COMPETITIVIDAD
REVISTA CIENTÍFICA Y TECNOLÓGICA

Vol. 24 No. 1-2022 - DOI: 10.25100/iyc.24i1.11063

SYSTEMS ENGINEERING

Evaluative study of an anonymous communication architecture for web browsing using SBC devices

INGENIERÍA DE SISTEMAS

Estudio evaluativo de una Arquitectura de comunicación anónima para la navegación web usando dispositivos SBC

Gustavo Alejandro Jiménez-Lagos[1§], Siler Amador-Donado[1], Katerine Márceles-Villalba[2]

[1]Universidad del Cauca, Facultad de Ingeniería Electrónica y Telecomunicaciones, Programa de Ingeniería de Sistemas, Grupo de investigación y desarrollo de Tecnologías de la Información (GTI), Popayán, Colombia

[2]Institución Universitaria Colegio Mayor del Cauca, Facultad de Ingeniería, Programa de Ingeniería Informática, Grupo de I+D en Informática, Popayán, Colombia

[§]*gajimene@unicauca.edu.co, samador@unicauca.edu.co, kmarceles@unimayor.edu.co*

Recibido: 7 de marzo de 2021 – **Aceptado**: 22 de julio de 2021

Abstract

The digital world brought many benefits and risks for users, consequently the need arises to protect the user's privacy while browsing the web, this article describes the evaluative study of the elements that are part of the architecture 6of a composite prototype by an SBC device and anonymity software that allows the user to keep their identity anonymous while browsing the web, initially, studies were carried out to determine which areas of communication to protect, which is the appropriate software for the architecture and which device to use for the prototype, additionally the corresponding performance tests to the prototype were carried out, in addition to the security tests based on the OWASP IoT project; Finally, the prototype developed allows anonymity by browsing from the operating system on the SBC device and also shares that anonymity through a Wi-Fi network so that users or external devices can connect.

***Keywords**: anonymity, anonymous browsing, privacy, simple computer board (SBC).*

Resumen

El mundo digital trajo muchos beneficios y riesgos para los usuarios, en consecuencia surge la necesidad de proteger la privacidad del usuario mientras navega por la web, en este artículo se describe el estudio evaluativo de los elementos que hacen parte de la arquitectura de un prototipo compuesto por un dispositivo SBC y software de anonimato que permite al usuario mantener anónima su identidad mientras navega por la web, inicialmente, se realizaron estudios

Como citar:
Jiménez-Lagos GA, Amador-Donado S, Márceles-Villalba K. Estudio evaluativo de una Arquitectura de comunicación anónima para la navegación web usando dispositivos SBC. INGENIERÍA Y COMPETITIVIDAD. 2022;24(1):e21411063. https://doi.org/10.25100/iyc.v24i1.11063.

para determinar qué áreas de la comunicación proteger, cuál es el software adecuado para la arquitectura y que dispositivo usar para el prototipo, adicionalmente se realizaron las correspondientes pruebas de rendimiento al prototipo, además de las pruebas de seguridad basados en el proyecto OWASP IoT; finalmente, el prototipo desarrollado permite el anonimato navegando desde el sistema operativo sobre el dispositivo SBC y además comparte ese anonimato por medio de una red Wi-Fi para que los usuarios o dispositivos externos puedan conectarse.

Palabras clave*: anonimato, navegación anónima, privacidad, placa sencilla de computador (SBC).*

1. Introduction

Living in today's interconnected world brings great benefits and threats. Apparently, the speed of communications and information exchange has opened new paths for the development of new technologies that were unimaginable a few years ago. However, along with the benefits this new world offers, significant new challenges arise. The same technology that allows families to communicate in real time across continents also enables the monitoring and cataloging of the contents of those conversations. In the same way, this technology allows online users to personalize their shopping experiences in such a way that they provide exactly what they want from the comfort of their home [(1)]. Consequently, anonymity is presented as the best protection tool for internet users. In the field of information technology and telecommunications, anonymous communication aims to hide the link between the sender and receiver of the communication, this includes the content of the message, the transmission route of the communication and the identities of the individuals, this it means that the content of the message is kept protected against external entities that want to access your information.

On the other hand, a growing technology is IoT or internet of things[(2)] which is accompanied by SBC devices[(3)] (single board computer). These are devices that have the main components of a computer fused into a single integrated circuit board, whose main characteristics are their reduced dimensions, their low cost, and their wide variety of devices on the market; because of this, their use has increased in recent years; Furthermore, many of these devices are based on the ARM architecture, which due to its simple instruction processing logic improves speed and reduces power consumption.

With respect to the above, the following research question arises, how to protect the communication channel to avoid information leakage in a web communications environment with the use of SBC devices?

For the development of this proposal, the research-action methodology was used, understanding it as a research approach characterized by the following: first, the researcher is a participating actor and the study phenomenon intervenes[(4)]; secondly, it is applied in a cyclical way, where each iteration allows a deeper understanding of the phenomenon; Finally, both the researcher and the participant mutually benefit from the process. Where, the researcher manages to better understand his study phenomenon, in this case to determine through an evaluative process the adequate anonymous communication architecture for web browsing using low-cost devices and free software and, on the other hand, the participant achieves solve a problem that affects them[(5)], which would be to be able to navigate safely, at low cost and portable, minimizing the risk of leaving a trace on the web.

2. Methodology

2.1 Hardware and software studies for the prototype

2.1.1 Study of tools for anonymous communication

The research and classification of the tools and methods that are currently used to control or maintain the anonymity of the user while browsing the network was carried out, followed by the grouping of these tools with respect to their field of implementation, obtaining the following areas:

1) Network security.
2) Anonymity-Oriented
3) Search engine privacy.
4) Instant messaging client.
5) Privacy in the browser.
6) Password management System.
7) Data encryption.

It should be noted that there are currently additional tools to those described in this section, for the realization of this selection of tools the following characteristics were taken into account: Mainly anonymity and privacy, in terms of operation tools with their stable versions and with system support, in licensing issues, tools with free software license were considered, free tools in their basic version with the possibility of increasing your privacy characteristics by buying a plus version, these selected tools have a good basic version that complies with the requirements for a user to maintain their privacy and anonymity.

Tool evaluation criteria: The objective of these criteria is to ensure an appropriate evaluation of each of the tools presented above, the following criteria are based considering the objectives proposed in this research. First, the characteristics that each of the tools must have were defined, in this case they were the following: anonymity, flexibility, ARM compatibility [(6)], costs and update period. Each tool has different specifications, and each specification has its corresponding value, that is, each characteristic provides a value that, when added together, finally generates the score for each tool. In the process of assigning values, it should be noted that the specifications of each characteristic are mutually exclusive except for the anonymity characteristic, which its specifications are inclusive depending on the tool, that is, a tool can comply with 1, 2, 3 or 4 anonymity specifications. Next, Table 1 shows the mentioned distribution

2.1.2 Results of the evaluation of tools

For the subsequent analysis of the results, the score obtained by each evaluated tool was transformed to its percentage value. These tools have 5 characteristics each one contributing with a maximum value established in the following way: Anonymity 5, because it's the main feature of the project, the following characteristics are: flexibility 1, compatibility 1, costs 1 and update period 1 that contribute a total of 4, that is, the maximum value that a tool could obtain is 9 that corresponds to 100%. Finally, the percentage and qualitative assessment was carried out to classify each of the tools evaluated as shown in the following Table 1.

Table 1. *Classification for each tool.*

Rating (%)	Qualitative
75 <x ≤ 100	Very high
50 <x ≤ 75	High
25 <x ≤ 50	Medium
0 <x ≤ 25	Low

Source: own elaboration

Next, Table 3 shows the results of the evaluation with the score obtained by each tool[(7)] and its corresponding percentage value, as well as the tools ordered from highest to lowest score in their corresponding area.

Tool evaluation analysis: For this study, a total of 29 tools were evaluated, 11 of which turned out to be not compatible with the ARM architecture, these are shown shaded (gray) in Table 2 in the compatibility column with the value of 0.

Table 2. *Tool evaluation criteria.*

Characteristic	Specification		Value	
Anonymity	**A1**	Techniques for concealing communication identifiers.	0 <x ≤ 1.25	$\sum_{i=0}^{4} Ai$
	A2	Communication content protection techniques.	0 <x ≤ 1.25	
	A3	Protection techniques for servers or communication nodes.	0 <x ≤ 1.25	
	A4	Protection techniques against network attacks.	0 <x ≤ 1.25	
Flexibility	**F1**	It does not allow to configure privacy.	0	
	F2	Allows you to configure privacy only for itself.	0.25	
	F3	Allows you to configure privacy for some network services.	0.5	
	F4	Allows you to configure privacy for all network services	1	
ARM Compatibility	**CA1**	It is not compatible.	0	
	CA2	It is supported and consumed as an external service.	0.5	
	CA3	It is supported and installed in the operating system.	1	
Costs	**C1**	It is completely paid.	0	
	C2	Free trial version only.	0.25	
	C3	Free basic version only.	0.5	
	C4	It is completely free.	1	
Update period	**P1**	Annual	0	
	P2	Biannual	0.25	
	P3	Monthly	0.5	
	Q4	Weekly	1	

Source: own elaboration

Table 3. *Evaluation of tools.*

Tool	**Anonymity**				**Flexibility**				**Compatibility**			**Costs**				**Period**				**Score**	**Percentage**
	A1	**A2**	**A3**	**A4**	**F1**	**F2**	**F3**	**F4**	**CA1**	**CA2**	**CA3**	**C1**	**C2**	**C3**	**C4**	**P1**	**P2**	**P3**	**P4**		
Network Tor	1.2	1.2	1	1.1	N/A	N/A	N/A	1	N/A	N/A	1	N/A	N/A	N/A	1	N/A	N/A	N/A	1	8.5	94.4
VPN	1	1.2	1	1	N/A	N/A	N/A	1	N/A	N/A	1	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	7.2	80.0
Network i2p	1	1.1	0.8	0.8	N/A	N/A	N/A	1	N/A	N/A	1	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	6.95	77.2
Proxy Server	0.8	0.7	0.6	0.7	N/A	N/A	N/A	1	N/A	N/A	1	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	5.8	64.4
Parrot	1.2	1.2	1	1.1	N/A	N/A	0.5	N/A	N/A	N/A	1	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	7.5	83.3
Qubes	1.2	1.2	1	1.2	N/A	N/A	N/A	1	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	7.1	78.9
Tails	1.2	1.2	1	1.1	N/A	N/A	N/A	1	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	7	77.8
Whonix	1.2	1.2	1	1	N/A	N/A	N/A	1	0	N/A	N/A	N/A	N/A	N/A	1	0	N/A	N/A	N/A	6.4	71.1
Duck Duck Go	0.2	0.4	0.5	0.1	0	N/A	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	N/A	N/A	N/A	1	3.7	41.1
Start Page	0.2	0.3	0.4	0.1	0	N/A	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	3	33.3
Gibiru	0.2	0.2	0.4	0.1	0	N/A	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	2.9	32.2
Torch	0.2	0.3	0.4	0.1	0	N/A	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	2.75	30.6
Onion Share	0.6	0.7	0.8	0.4	N/A	0.25	N/A	N/A	N/A	N/A	1	N/A	N/A	N/A	1	N/A	N/A	N/A	1	5.75	63.9
Proton Mail	0.6	0.7	1	0.4	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	4.95	55.0
Ricochet	0.6	0.5	0.5	0.2	N/A	0.25	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	N/A	1	4.05	45.0
Onion Mail	0.6	0.5	0.6	0.4	N/A	0.25	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	3.85	42.8
Paranoid	0.6	0.7	0.5	0.2	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	3.75	41.7
Browser Tor	1.1	1.2	0.9	0.9	N/A	N/A	0.5	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	6.1	67.8
Browser EPIC	1	1	0.8	0.9	N/A	N/A	0.5	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	5.7	63.3
Midori	0.4	0.4	0.3	0.3	N/A	N/A	0.5	N/A	N/A	N/A	1	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	4.15	46.1
Brave	0.6	0.6	0.6	0.4	N/A	N/A	0.5	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	3.95	43.9
Last Pass	0.5	0.8	0.4	0.6	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	4.55	50.6
Dash Lane	0.5	0.7	0.4	0.5	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	4.35	48.3
Password	0.5	0.6	0.4	0.5	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	4.25	47.2
Keeper	0.5	0.5	0.4	0.4	N/A	0.25	N/A	N/A	N/A	0.5	N/A	N/A	N/A	0.5	N/A	N/A	N/A	N/A	1	4.05	45.0
VeraCrypt	N/A	1	N/A	0.3	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	3.55	39.4
BitLocker	N/A	1	N/A	0.3	0	N/A	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	N/A	0.5	N/A	2.8	31.1
AxCrypt	N/A	0.9	N/A	0.3	0	N/A	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.5	N/A	2.2	24.4
ZuluCrypt	N/A	0.7	N/A	0.2	0	N/A	N/A	N/A	0	N/A	N/A	N/A	N/A	N/A	1	N/A	0.25	N/A	N/A	2.15	23.9

Source: own elaboration

For this reason, these tools were discarded for the development of this project; However, it should be noted that they are tools that provide a high level of anonymity, since they have been specifically designed with the aim of maintaining privacy on the network and are tools commonly used by people whose job or occupation requires the protection of their identity such as: journalists, politicians, government agents, among others.

Next, from Table 4, it can be seen how the Tor project is present in 2 of the 5 tools in the ranking (rows 1 and 2), taking into account that the Parrot operating system uses the Tor network internally to route its traffic; On the other hand, the presence of cryptographic methods that protect the content of the communication can be implicitly noticed, in addition they hide the true IP address of the user and protect the privacy of the communication route, finally, in the area called security of The network has the largest number of tools positioned in the top 5 (previous table 4) compared to the other areas, in other terms, network security 4 and anonymous operating systems 1.

Table 4. *Top 5 of the tools*

Nº	Tool	Score	Percentage	Qualitative
1	Network Tor	8.5	94.4	Very high
2	Parrot	7.5	83.3	Very high
3	VPN	7.2	80.0	Very high
4	I2P network	6.95	77.2	Very high
5	Proxy Server	5.8	64.4	Very high

Source: own elaboration

As mentioned before, each tool was grouped depending on its implementation area, this was done because each of the tools provides privacy to a certain area of the user who browses through cyberspace[8], in addition to this, each tool operates in a different way and provides a different level of anonymity, thinking about protecting each aspect of the user, the selection of the best tool by area was made as shown in the following Table 5, it should be remembered that the tools incompatible with the ARM architecture were discarded.

According to Table 5, for the parameters of this study and the requirements of this project, the set of tools presented, are the best option for a user to keep their identity anonymous on the network, in conclusion, to achieve anonymity it must be managed the security of each aspect or area involved in the communication since the smallest information leak can cause a domino effect that ultimately causes loss of private information or exposure of real user data. It should be noted that the selected tools have no financial cost for their implementation.

2.2 Low-cost SBC device study

2.2.1 SBC device characterization

For the development of the solution of this research work it is desired to build a low-cost hardware prototype based on SBC devices [9], for this reason a search was made of the devices that are currently on the market. It should be noted that all the devices classified are of RISC (Reduced Instruction Set Computer) architecture on which the ARM microprocessors are based, in addition the price value is an approximate that covers the cost of the device and its shipping as a reference, this classification was made with the devices offered until July 20, 2019.

2.2.2 Device evaluation results

For the analysis of the results, the score obtained from each device was transformed into its percentage value, in other words, each characteristic provides a maximum value of 1, therefore, the maximum score that a device could obtain is 6, which represents 100 %, for this study the devices with the highest percentage are those considered suitable for this research, finally, the percentage and qualitative assessment was

Table 5. *The best tool in each area.*

Area	Tool	Score	Percentage	Qualitative
Network security	Network Tor	8.5	94.4	Very high
Anonymous operating systems	Parrot	7.5	83.3	Very high
Privacy in the search engine	Duck Duck Go	3.7	41.1	Medium
Instant messaging client	OnionShare	5.75	63.9	High
Privacy in the browser	Midori	4.15	46.1	Medium
Password management client	LastPass	4.55	50.6	High
Data encryption	VeraCrypt	3.45	38.3	Medium

Source: own elaboration

established that classifies each of the devices evaluated as shown in the following Table 6. Next, Table 7 presents the evaluation and the results obtained by each device with its corresponding score and percentage valuation ordered from highest to lowest.

Table 6. *Percentage and qualitative valuation of devices.*

Rating (%)	Qualitative
75 <x ≤ 100	Very high
50 <x ≤ 75	High
25 <x ≤ 50	Medium
0 <x ≤ 25	Low

Source: own elaboration

Device evaluation analysis: The objective of this study is to find the devices that best fit the project requirements, taking into account the following aspects: *Performance:* the device must have the ability to execute processes quickly and in parallel, in the same way it is obliged to load a complete operating system in addition to additional tools similar or equal to those presented in the previous study. *Support:* the device should have as much documentation and software support as possible, due to the diverse number of tools that have been developed with a focus on cybersecurity. *Price:* the device must have the lowest possible cost while maintaining a balance regarding the two aspects mentioned above.

The Raspberry pi [(10)] foundation is currently an organization with years of experience dedicated to the production of SBC devices, among them are the Raspberry pi 3 and 4 devices that managed to position themselves in the top 5 of devices considered suitable for the implementation of the prototype (Table 8), also with very close scores followed by the Rock pi, Orange pi and Latte. panda devices manufactured by Chinese organizations that have several years dedicated to the creation of hardware solutions, in conclusion, any of the five devices presented above are considered a good choice and that meet the requirements of the project, also come from trusted entities with experience in the development of these hardware devices.

2.3 Study of operating systems for SBC devices

Previously, in section 2.1.1 study of tools for anonymous communication, some dedicated operating systems were presented specifically to meet the anonymity requirements of an online user, later on, performing the analysis of the results, those that were not compatible were

Table 7. *Evaluation of the devices.*

Devices	Price	Processor		RAM	Module	Support	Score	Percentage
		Nucleus	Frequency					
Raspberry Pi 3	0.66	0.5	1	0.25	1	1	4.41	73.5
Raspberry Pi 4	0.32	0.5	0.5	1	1	1	4.32	72.0
Rock Pi 4	0.51	0.5	1	0.5	1	0.5	4.01	66.8
Orange Pi Plus 2E	0.47	0.5	1	0.5	1	0.5	3.97	66.1
Latte Panda	0.16	0.5	1	0.5	1	0.5	3.66	61.0
Pine A64 LTS	0.62	0.5	0.5	0.5	1	0.5	3.62	60.3
Ordroid C2	0.56	0.5	0.5	0.5	1	0.5	3.56	59.4
Asus Tinker Board S	0.43	0.5	1	0.5	1	0	3.43	57.1
Banana Pi M2	0.62	0.5	0.25	0.25	1	0.5	3.12	52.0
Raspberry Pi Zero	0.72	0	0.25	0	1	1	2.97	49.6
Orange Pi PC	0.71	0.5	0	0.25	1	0.5	2.96	49.4
Nano Pi R1	0.70	0.5	0.5	0.25	0	0.5	2.45	40.8
Dragon Board	0.15	0.5	0.5	0.25	1	0	2.40	40.0
nVidia Jetson TK1	0.00	0.5	0.5	1	0	0	2.00	33.3
Beagle Bone Black	0.47	0	0.25	0	1	0	1.72	28.6
Wand Board Dual	0.22	0.25	0.25	0.25	0	0	0.97	16.2

Source: own elaboration

Table 8. *Top 5 SBC devices.*

Nº	Device	Score	Percentage	Qualitative
1	Raspberry pi 3	4.41	73.5	High
2	Raspberry pi 4	4.32	72.0	High
3	Rock pi 4	4.01	66.8	High
4	Orange pi plus 2E	3.97	66.1	High
5	Panda latte	3.66	61.0	High

Source: own elaboration

discarded, leaving as a result the Parrot operating system, the main objective of this section is to present other compatible operating systems that Can be added to the project solution, in other words, operating systems that allow the implementation of a prototype that meets all the software requirements and that additionally, make the best use of the hardware resources of the SBC device.

2.3.1 Results of the evaluation of operating systems

For the analysis of the results, the result of the score obtained from each operating system was transformed into its percentage value to easily and clearly manage the data obtained in the evaluation, in this way it is necessary that each characteristic contributes a maximum value of 1, for Therefore, the maximum score that an operating system could obtain is 5, which represents 100%, for this study the operating systems with the highest percentage are those considered suitable for the project, finally, the percentage and qualitative assessment that classifies each one of the systems evaluated as shown in the following Table 9. Next, Table 10 shows the evaluation and the results obtained by each operating system with its corresponding score and percentage valuation ordered from highest to lowest.

Table 9. *Percentage and qualitative assessment of operating systems.*

Rating (%)	Qualitative
75 <x ≤ 100	Very high
50 <x ≤ 75	High
25 <x ≤ 50	Medium
0 <x ≤ 25	Low

Source: own elaboration

Analysis of the evaluation of operating systems: The objective of this study of operating systems is to identify which are the best options to be implemented in the final solution, all this taking into account the characteristics presented above that allow in the evaluation to maintain a balance between the performance of the hardware and the reliability of the operating system for implementation of this research work, below, Table 11 lists the 5 operating systems that obtained the best scores in the evaluation. With respect to the results obtained in the previous Table 11, the following statement can be extracted. The Debian operating system is implicitly shown as the best option to be implemented in the solution, since it is present in each of the operating systems except for Alpine Linux, which was developed based on other libraries, keeping in mind that Raspbian and DietPi They have been developed based on Debian Buster, finally Ubuntu Mate belongs to one of the many Debian distributions.

2.4 Study of controls and security tests

2.4.1 Security controls for network communications

Below are the controls that must be implemented to guarantee information security in a network communications environment according to the ISO 27002 standard of 2013(11). This standard is divided by 14 domains and 114 controls with their corresponding names, the domains refer to the area that is going to be managed and the controls are the guidelines that must be met to maintain the security of the information. Based on the objectives of this project, domains 10 and 13 apply, which refer respectively to cryptography and communications security.

OWASP IoT project

The OWASP Internet of Things Project(12), started in 2014, is designed to help manufacturers, developers and consumers better understand the security issues associated with IoT (Internet of Things), and to allow users in any context to make better security decisions by build, implement or evaluate IoT technologies, the most recent OWASP IoT testing guide corresponds to the OWASP IoT Top 10 of the year 2018(12). The project seeks to define a structure for several IoT sub-projects separated into the following 10 categories.

Table 10. *Evaluation of operating systems.*

Operating Systems	Memory resources		Support	Period	Costs	Score	Percentage
	RAM	ROM					
Raspbian Buster Lite	0.94	0.48	1	1	1	4.42	88.33
Raspbian Buster	0.41	0.28	1	1	1	3.69	73.78
DietPi	0.95	0.76	0.25	0.5	1	3.47	69.30
Alpine Linux	0.92	0.76	0.25	0.25	1	3.18	63.69
Ubuntu Mate	0.38	0.18	0.5	1	1	3.05	61.00
Risc OS	0.89	0.53	0	0.5	1	2.92	58.35
Pipa OS	0.93	0.55	0.25	0	1	2.73	54.63
Windows IoT Core	0.59	0.63	1	0.25	0.25	2.71	54.30
Open Media Vault	0.88	0.30	0.25	0.25	1	2.68	53.66
Windows IoT Enterprise	0.51	0.45	1	0.5	0	2.46	49.23

Source: own elaboration

Table 11. *Top 5 operating systems.*

Do not	Operating system	Score	Percentage	Qualitative
1	Raspbian Buster Lite	4.42	88.3	Very high
2	Raspbian buster	3.69	73.78	High
3	DietPi	3.47	69.30	High
4	Alpine Linux	3.18	63.7	High
5	Ubuntu Mate	3.05	61.0	High

Source: own elaboration

OWASP IoT Security Testing Guide

The guide below is at a basic level, giving device and app testers a set of guidelines to consider from their perspective. This is not an exhaustive list of considerations and should not be treated as such, but ensuring these fundamentals are covered will greatly enhance the security of any IoT product. The categories covered by the test are listed below: I1- Insecure web interface, I2- Insufficient authentication or authorization, I3- Insecure network services, I4- Lack of transport encryption, I5- Privacy concerns, I6- Cloud interface Insecure, I7- Insecure Mobile Interface, I8- Insufficient Security Configuration, I9- Insecure Software or Firmware, and I10- Bad Physical Security.

Study and evaluation of configurations for the prototype

Based on the results obtained in the three previous studies where tools, SBC devices and operating systems were evaluated, the configurations presented in the following Table 12 were elaborated, it is worth mentioning that these are only initial proposals to build the final solution, this because Compatibility problems between the operating system and the tools can probably arise, in addition it is intended to build a prototype that preserves a balance between hardware performance and its functionality given that there are limited machine resources due to each SBC device.

It is important to note that configuration 4 highlighted in light gray has a fixed configuration because Parrot as an operating system contains pre-configured tools by default, among them are the Tor network, Duck duck go, Onionshare, Tor browser and ZuluCrypt, in addition, it contains some few tools that were presented in section 2.1.1 study of tools for anonymous communication and a great variety of additional tools related to security, anonymity, pentesting, among other areas.

2.4.2 Evaluation of configurations

Configuration evaluation criteria

The following criteria were established to determine which of all is the appropriate configuration to continue with the construction of the prototype, taking as a reference the requirements of this investigation. First, the characteristics with which each configuration must comply were defined, in this case they were the following: Anonymity, Performance, Protected Area and OWASP IoT. Each configuration has its specifications, and each specification has its corresponding value, that is, each characteristic contributes a value that when added together finally generates the score for the configuration. It should be noted that in the anonymity characteristic its specifications are inclusive depending on the selected configuration. In other words, a configuration can meet A1, A2, A3, or A4 specifications for that characteristic.

Anonymity has 4 specifications that in this case evaluate the security of the area called "Network Security" and correspond to the same specifications established in the study of tools. The Protected Area has 5 specifications that correspond to the remaining 5 areas (excluding "Anonymous operating systems") in other words it is the number of areas that the configuration protects. The Performance corresponds to the RAM memory resources (including buffer and cache) that each configuration needs to keep the operating system running with its anonymity tools in its active or working state, in other terms, the greater the available memory space, the greater it is. the score, it is necessary to clarify that all these memory tests were carried out using the same hardware device, for these tests, the "most limited case" of the top 3 devices was selected, that is, the Raspberry Pi 3 board because it is the device with the lowest RAM capacity (1GB) compared to the other devices.

With this "more limited case" it was verified that it’s possible to execute each of the configurations. The OWASP IoT characteristic corresponds to the tests developed by the OWASP IoT project, the configurations were evaluated considering each of the tests established in the OWASP IoT project, that is, the value obtained by a configuration is given by the total amount of tests passed, the total number of OWASP IoT tests is 50 and in this case each test passed contributes 0.1 to the final value. Next, Table 13 shows the mentioned distribution

Results of the configuration evaluation

For the analysis of these results, the score obtained for each configuration evaluated was transformed to its percentage value to classify it as shown in the following Table 14, for this evaluation 5 characteristics presented previously were determined, each one providing a maximum value established for the following form: Anonymity 5, Protected Area 5, Performance 5 and OWASP IoT 5, that is to say that the maximum value that a configuration could obtain is 20 which corresponds to 100%, with this assessment it is possible to determine what configuration or configurations are appropriate for this project, maintaining a balance between its main characteristic, which is anonymity, the areas that it manages to anonymize and the performance of the CPU, since SBC devices have limited hardware capabilities, and must also pass the

Table 13. *Configuration evaluation criteria.*

Characteristic	Specification		Value	
Anonymity	**A1**	Techniques for concealing communication identifiers.	0 <x ≤ 1.25	$\sum_{i=0}^{4} Ai$
	A2	Communication content protection techniques.	0 <x ≤ 1.25	
	A3	Protection techniques for servers or communication nodes.	0 <x ≤ 1.25	
	A4	Protection techniques against network attacks.	0 <x ≤ 1.25	
Protected area	**P1**	Privacy in the search engine	x = 1	$\sum_{i=0}^{5} APi$
	P2	Instant messaging client	x = 1	
	P3	Privacy in the browser	x = 1	
	Q4	Password management client	x = 1	
	P5	Data encryption	x = 1	
Performance	Value 0 = no memory available. Value 5 = 100% of memory is available.		0 <x ≤ 5	
OWASP IoT	Number of OWASP IoT tests passed. Totality of tests = 50 Value per approved test = 0.1		0 <x ≤ 5	

Source: Author's own

largest number of tests designed, by the OWASP IoT project, for this type of project or prototype. Finally, we proceed with the percentage and qualitative assessment to classify each of the configurations evaluated as shown in the following Table 14.

Table 14. *Classification for each configuration.*

Rating (%)	Qualitative
75 <x ≤ 100	Very high
50 <x ≤ 75	High
25 <x ≤ 50	Medium
0 <x ≤ 25	Low

Source: own elaboration

Next, Table 15 presents the results of the evaluation with the score obtained for each configuration and its corresponding percentage value, as well as the tools ordered from highest to lowest score in their corresponding area.

Configuration analysis and selection: With respect to the data presented in Table 15, the following conclusions can be drawn: In the Anonymity characteristic, when adding their values for each configuration, it is obtained that C2 and C4 achieve the best score (4.5) compared to the other configurations (4.2), this is because C2 and C4 use Tor as an anonymity service for the network compared to the others that use a VPN, this score is higher thanks to the extra

Table 15. *Evaluation of the configurations.*

Setting	Anonymity				Protected area					Performance	Owasp IoT	Score	Percentage	Qualitative
	A1	A2	A3	A4	P1	P2	P3	P4	P5					
C1	1	1.2	1	1	N/A	1	1	N/A	1	4	2.2	13.4	67.0	High
C2	1.2	1.2	1	1	1	1	1	A	1	3.2	3.5	16.2	81.0	Very High
C3	1	1.2	1	1	N/A	N/A	1	N/A	1	4.7	2.1	13	65.0	High
C4	1.2	1.2	1	1	1	1	1	1	1	1.5	3.6	14.6	73.0	High

Source: own elaboration

protection that the Tor network has by managing to hide the communication path and use an encryption system that allows to protect the communication content with its original location in a better way than the VPN, in addition with the Protected Area feature it can be noticed as the C2 and C4 configurations because of its operating system allow to protect all areas that may be vulnerable to the user (score 5).

The above is presented as a disadvantage when compared to the Performance feature where C2 and C 4 have the lowest score in this column, this is because C1 and C3 (i.e. Raspbian Buster Lite and DietPi) are systems specifically designed to make optimal use of the machine resources of the SBC device, because of this the system has some limitations of use that do not allow protecting all areas of a user's communication as seen in the Protected Area column where C1 and C3 obtained low scores, additionally these limitations also affected their scores obtained in the OWASP IoT column where they could not be apply many of the tests due to the absence of interface (categories I1 and I7).

Finally, the configuration chosen to continue with the development of the project was C2, which obtained the highest score as seen in Table 15, then in Table 16 this configuration C2 is presented with its corresponding tools.

Table 16. *Configuration selected for the prototype.*

Area	C2
Operating system	Raspbian buster
Network security	Red Tor
Privacy in the search engine	Duck Duck Go
Instant messaging client	ProtonMail
Privacy in the browser	Midori
Password management client	LastPass
Data encryption	VeraCrypt

Source: own elaboration

3. Prototype evaluation

3.1 Prototype evaluation criteria

The evaluation of the prototypes was carried out using the first two devices of the top 5 of SBC devices, that is, Raspberry PI 3 and Raspberry PI 4, the Rock PI 4 device was not evaluated, because it has similar characteristics to the Raspberry PI 4 and additionally, it presents a limitation, which is its delivery time in Colombia, which is 4 to 6 weeks, and the schedule affected us.

The main evaluation criteria for these two devices are Performance and Security, with respect to device performance, the percentage of RAM available in two specific scenarios was determined, scenario 1 is when the default configuration is used, that is, when the device is only used as an anonymous router for clients to connect to the anonymous network, scenario 2 is when the client wants to additionally use the tools configured in the system such as: the password manager, the messaging client between Others, with respect to the security criteria, it was evaluated that each prototype complies with the security controls presented in section. ***Security controls for network*** communications and additionally that it complies with the security tests defined by the OWASP project presented in section ***OWASP IoT security tests***, finally the Cost of each device was included.

4. Conclusions

The evaluation of the prototypes was carried out using the first two devices of the top 5 of SBC devices, that is, Raspberry PI 3 and Raspberry PI 4, the Rock PI 4 device was not evaluated, because it has similar characteristics to the Raspberry PI 4 and additionally, it presents a limitation, which is its delivery time in Colombia, which is 4 to 6 weeks, and the schedule affected us. The main evaluation criteria for these two devices are Performance and Security, with respect to device performance, the percentage of RAM available in two specific scenarios was determined, scenario 1 is when the default configuration is used, that is, when the device is only used as an anonymous router for clients to connect to the anonymous network.

In scenario 2, the difference in memory is evident, since when using the five tools at the same time, the Raspberry PI 3 is left with 3% of memory, which affects the response speed of the system, making operations very delayed and sometimes it can cause the system to hang, in this case the performance of the system was maintained and is established using a maximum of 2 tools at the same time, this does not happen with the Raspberry PI 4 which, having the same workload, works correctly and keeps available more than half the memory so the system can perform other operations. With regard to safety, the two prototypes comply with all the controls set out in section **2.4.2**, In relation to the OWASP IoT security tests, the prototypes comply with the 35 tests that are allowed to be executed for this configuration (C2); Finally, there is the cost relationship between the devices, which is a personal decision criterion, since it is the person or the client who decides which prototype to use depending on the way they need to use the service. Likewise, it is highlighted that this is a very low-cost option that can be always used due to its portability and use of free software, characterized by being able to minimize the risk of leaving traces of the data that are handled when browsing the web and reduce the possibility of leaving the information being transferred vulnerable.

5. Acknowledgment and funding statement

Thanks to the Universidad del Cauca, especially to its GTI research group and to the Computer Research and Development Group (Computer R&D) of the Institución Universitaria Colegio Mayor del Cauca, for the support provided in terms of financing for the development of the project.

6. References

(1) Freedman M. How Businesses Are Collecting Data (And What They're Doing With It). Business News Daily. [Internet]; 2020 [cited: 2020 02 07]. Available from: https://n9.cl/ocwbd.

(2) Mendieta T, Herrera J, Jiménez A. La Capacidad del IOT de Transformar el Futuro. Revista AVENIR. 2019 09 18;1(1):15-18. Available from: https://fundacionavenir.net/revista/index.php/avenir/article/view/79.

(3) Vázquez DJ, Reigosa L. Una nueva aproximación a la enseñanza tecnológica superior de informática centrada en

dispositivos de computación de bajo costo y alto rendimiento. In: Memorias del primer Congreso Internacional de Ciencias Pedagógicas. Guayaquil: Instituto Superior Tecnológico Bolivariano de Tecnología; 2015. p. 596–609.

(4) Greenwood D, Levin M. Introduction to Action Research. In: 2nd ed. Thousand Oaks C. Social Research for Social Change. Sage Publications Inc. 2007. https://dx.doi.org/10.4135/9781412984614

(5) Kock NF, McQueen RJ, John LS. Can action research be made more rigorous in a positivist sense? The contribution of an iterative approach. Journal of Systems and Information Technology. 1997;1(1):1-23. https://doi.org/10.1108/13287269780000732

(6) Moreno S, Rodriguez A, Sarmiento Y.Supercomputación basada en arquitectura ARM [Internet]. Bucaramanga: Universidad Industrial de Santander [cited 2021 feb 15]. Available from: http://wiki.sc3.uis.edu.co/images/1/12/G11.pdf.

(7) Zúñiga M, Amador D, Márceles K. Protección de datos anónima y portable. 1st ed. Popayán: Editorial Académica Española; 2020.

(8) Sanz F. Estudio de tecnologías para la protección de la privacidad mediante anonimato. [Bacherlor’s Degree]. Madrid: Universidad Autónoma de Madrid;2018. Available from: https://repositorio.uam.es/bitstream/handle/10486/688072/andreu_sanz_francisco_tfg.pdf?sequence=1.

(9) Pantoja ND, Jiménez AF, Donado SA, Márceles K. Cryptanalysis of the RSA Algorithm Under a System Distributed Using SBC Devices. In: Mata-Rivera M, Zagal-Flores R, editors. Telematics and Computing WITCOM 2018 Communications in Computer and Information Science, vol 944. Springer, Cham; 2018. p. 3–12. https://doi.org/10.1007/978-3-030-03763-5_1

(10) Zúñiga M, Amador D, Márceles K. Servicio de navegación anónima basada en un–Raspberry Pi. Revista íberica de Sistemas y Tenologías de la información. 2019 Dec;(26):587-597.

(11) The International Organization for Standardization-ISO/IEC JTC 1/SC 27 Information security, cybersecurity and privacy protection. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls. 2nd ed. Switzerland: The International Organization for Standardization-ISO; 2013. Available from: https://www.iso.org/standard/54533.html

(12) The OWASP Foundation. OWASP Internet of Things. [Internet].; 2018. [cited 2020 02 14] Available from: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project.