



Universidad Autónoma de San Luis Potosí
Facultad de Ingeniería
Centro de Investigación y Estudios de Posgrado

Cyberattacks Study and Framework in Brain-Computer Interfacing Devices

Que para obtener el grado de:

Maestría en Ingeniería de la Computación

Presenta:

Antonio de Jesús Menchaca Martínez

Asesora:

Dra. Alejandra Guadalupe Silva-Trujillo

San Luis Potosí, S. L. P.

Noviembre de 2025



Abstract

Advanced neurotechnologies, particularly Brain-Computer Interfaces (BCIs), are revolutionizing human- machine interactions, providing remarkable advancements across medical, industrial, educational, entertainment, and security domains. Despite BCIs' great potential, they simultaneously raise critical ethical concerns regarding user data privacy and their Neuro Rights, which aim to safeguard individuals against the risks of emerging neurotechnologies, especially as they become increasingly available on the market. Utilizing a comprehensive literature review and implementing a passive attack on two commercial BCI devices, the study reveals critical vulnerabilities during all the phases of the system. Our findings underscore the urgent need for robust cybersecurity frameworks, including Privacy-by-Design strategies. To address this problem, we designed a scoring framework based on the Bluetooth standard, that guides manufacturers and helps regulators, guaranteeing the safe adoption of BCIs. The proposed solution aims to enhance the security of the pairing process on BCI devices, thereby ensuring user neural data integrity and protection.

Resumen

Las neurotecnologías avanzadas, en particular las Interfaces Cerebro-Computadora (BCIs), están revolucionando la interacción humano-máquina, ofreciendo avances notables en los ámbitos médico, industrial, educativo, del entretenimiento y de la seguridad. A pesar del enorme potencial de las BCIs, estas tecnologías plantean simultáneamente importantes preocupaciones éticas relacionadas con la privacidad de los datos de los usuarios y sus Neuroderechos, cuyo objetivo es proteger a las personas frente a los riesgos de las neurotecnologías emergentes, especialmente a medida que se vuelven cada vez más accesibles en el mercado. Mediante una revisión exhaustiva de la literatura y la implementación de un ataque pasivo sobre dos dispositivos BCI comerciales, el estudio revela vulnerabilidades críticas en todas las fases del sistema. Nuestros hallazgos subrayan la necesidad urgente de marcos sólidos de ciberseguridad, incluidos enfoques de Privacidad desde el Diseño (Privacy-by-Design). Para abordar este problema, diseñamos un marco de puntuación basado en el estándar Bluetooth, que orienta a los fabricantes y ayuda a los reguladores, garantizando una adopción segura de las BCIs. La solución propuesta busca mejorar la seguridad del proceso de emparejamiento en dispositivos BCI, asegurando así la integridad y protección de los datos neuronales de los usuarios.



18 de septiembre de 2025

**DRA. ALEJANDRA GUADALUPE SILVA TRUJILLO
P R E S E N T E.**

Por este conducto, me permito informarle, que en sesión ordinaria del H. Consejo Técnico Consultivo celebrada el día 18 de septiembre del presente, fue analizada y aprobada su petición en la cual solicita autorización para que el **Ing. Antonio de Jesús Menchaca Martínez** de la **Maestría en Ingeniería de la Computación**, se titule mediante la modalidad: **Artículo Científico**, con el artículo denominado:

"Estudio de Ciberataques y Privacidad en Dispositivos de Interfaz Cerebo-Computadora (Cyberattacks Study and Privacy in Brain-Computer Interfacing Devices)"

Al respecto me permito informarle, que de acuerdo a su colaboración y en la publicación del artículo antes mencionado, ha sido propuesta como Asesora.

Sin otro particular de momento, quedo de usted.

"MODOS ET CUNCTARUM RERUM MENSURAS AUDEBO"

A T E N T A M E N T E

**DR. RICARDO ROMERO MÉNDEZ
SECRETARIO DEL CONSEJO.**

UNIVERSIDAD AUTÓNOMA DE SAN LUIS POTOSÍ
FACULTAD DE INGENIERÍA
SECRETARÍA

www.uaslp.mx

Av. Manuel Nava 8
Zona Universitaria • CP 78290
San Luis Potosí, S.L.P.
tel. (444) 826 2330 al39
fax (444) 826 2336

Ccp. **Ing. Antonio de Jesús Menchaca Martínez.**
Archivo.
-bvlg

"1945-2025: 80 años formando profesionales de la Ingeniería en beneficio de la sociedad"

Table of Contents

Paper	6
Presentation	13
A Cyberattacks Study and Privacy in Brain-Computer Interfacing Devices.....	27
A.1 Introduction.....	28
A.2 BCI Applications and User Privacy.....	31
A.3 BCI Communication Protocols	32
A.4 BCI Vulnerabilities and Challenges	33
A.5 Bluetooth Low-Energy Pairing Methods.....	36
A.6 Passive Attack Test.....	37
A.7 Scoring Framework.....	39
A.8 Conclusions and Final Thoughts.....	42
References.....	42

Chapter 1

Paper

This chapter contains the acceptance letter for the “*XL Simposio Nacional de la Unión Científica Internacional de Radio (URSI 2025)*” and then the paper submitted to the conference.

Antonio de Jesús Menchaca Martínez
UPPA
STEE
10 allées des Cèdres, Appt B54
64600 Anglet
Francia

10/09/2025

Estimado/a Sr. o Sra.

Esta carta confirma que **Antonio de Jesús Menchaca Martínez** es autor/co-autor de una o más contribuciones presentadas en el **XL Simposio Nacional de la Unión Científica Internacional de Radio (URSI 2025)**, celebrado en Tarragona, del 3 al 5 de Septiembre de 2025.

Antonio de Jesús Menchaca Martínez es autor/coautor de la(s) siguiente(s) contribución(es):

Cyberattacks Study and Framework in Brain-Computer Interfacing Devices

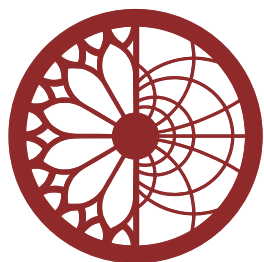
Autor(es): Menchaca-Martínez, Antonio de Jesús; Silva-Trujillo, Alejandra Guadalupe; Arjona-Villicaña, Pedro David

Ponente: Menchaca-Martínez, Antonio de Jesús

Estado: Su contribución ha sido aceptada

El comité organizador del congreso le agradece su participación.

Un saludo cordial,



URSI 2025
TARRAGONA
XL Simposio Nacional de la Unión
Científica Internacional de Radio



D. David Girbau Sala y D. Antonio Lázaro Guillén, presidentes del comité organizador y científico del XL Simposio Nacional de la Unión Científica Internacional de Radio, URSI 2025 - Tarragona

CERTIFICAN QUE:

Antonio de Jesús Menchaca Martínez

Ha asistido al XL Simposio Nacional de la Unión Científica Internacional de Radio celebrado en formato presencial durante los días 3, 4 y 5 de septiembre de 2025 en el Palacio Ferial y de Congresos de Tarragona.

En Tarragona, 5 de septiembre de 2025.

David Girbau Sala

Antonio Lázaro Guillén



Cyberattacks Study and Framework in Brain-Computer Interfacing Devices

Antonio de Jesús Menchaca-Martínez⁽¹⁾, Alejandra Guadalupe Silva-Trujillo⁽²⁾, Pedro David Arjona-Villicaña⁽²⁾

adjmmartinez@univ-pau.fr, asilva@uaslp.mx, david.arjona@uaslp.mx

⁽¹⁾ Collège STEE, Université de Pau et des Pays de l'Adour (UPPA), Anglet, France.

⁽²⁾ Facultad de Ingeniería, Universidad Autónoma de San Luis Potosí (UASLP), San Luis Potosí, México

Abstract— Brain-Computer Interfaces (BCIs), are revolutionizing human-machine interactions, providing remarkable advancements across medical, industrial, educational, entertainment, and security domains. Despite BCIs' great potential, they simultaneously raise critical ethical concerns regarding user data privacy and their Neurorights, which aim to safeguard individuals against the risks of emerging neurotechnologies, especially as they become increasingly available on the market. Utilizing a comprehensive literature review and implementing a passive attack on two commercial BCI devices, the study reveals critical vulnerabilities during all the phases of the system. Our findings underscore the urgent need for robust cybersecurity frameworks, including Privacy-by-Design strategies. To address this problem, we designed a scoring framework based on the Bluetooth standard, that guides manufacturers and helps regulators, guaranteeing the safe adoption of BCIs. The proposed solution aims to enhance the security of the pairing process on BCI devices, thereby ensuring user neural data integrity and protection.

Keywords— Neurorights, BCIs, cybersecurity, neural data privacy, BLE.

I. INTRODUCTION

Brain-Computer Interfaces (BCIs) are a neurotechnology that enables communication and control between users and computer systems beyond traditional keyboard-based interaction. They do not rely on any other external devices nor human intervention (i.e., muscular or speech) to complete an intended task, such as controlling a robotic arm or restoring motor function in individuals with spinal cord injuries [1]. Furthermore, BCIs can also provide a real-time communication between the brain and external digital devices through brain-to-internet (B2I) connectivity [2]. With the adoption of 6G technology, that promises ultra-low latency and massive connectivity, the integration of BCIs into everyday applications is expected to accelerate, requiring a reassessment of cybersecurity frameworks to protect increasingly interconnected neural devices.

Commercial BCIs operate by acquiring neural signals and, in more specialized implementations, delivering neural stimulation to modulate brain activity. This forms a closed feedback loop essential for device operation [3]. Brain activity can be measured using different hardware technologies, which can be classified into invasive and non-invasive techniques. Non-invasive techniques include Electro Encephalo Graphy (EEG), Magneto Encephalo Graphy (MEG), functional Magnetic Resonance Imaging (fMRI), and functional Near InfraRed Spectroscopy (fNIRS). Invasive techniques comprise Electro Cortico Graphy (ECOG) and Subcortical Electrode Arrays (SEA). Notably,

the majority of BCIs rely on EEG technology to record the electrical fields generated by neuronal synaptic activity. Due to its portability and affordability.

This paper focuses on the vulnerabilities that BCIs face during the pairing process, primarily due to their reliance on Bluetooth. It reviews the evolution and privacy issues of BCIs on Section II, identifies current communication protocols and pairing methods on Section III, and systematically analyzes vulnerabilities and challenges from the literature on Section IV. It then details Bluetooth Low Energy (BLE) pairing methods on Section V, demonstrates a passive attack on two devices on Section VI, introduces a scoring framework for security requirements on Section VII, and concludes with overall findings and proposals on Section VIII.

II. BCI APPLICATIONS AND USER PRIVACY

Since its origins in the 1970's, Brain-Computer Interfaces (BCIs) have primarily served healthcare, assisting individuals with severe disabilities and advancing diagnostics, treatment, and rehabilitation [3]. Over time, BCIs have expanded their scope into diverse non-medical fields such as neuroergonomics (smart homes, workplaces), neuromarketing (advertisements), education (skill learning with fMRI), gaming (VR-based interaction), and security (biosignal-based authentication) [4]. Furthermore, new technologies like Neuralink implanted its first device in a human subject.

While the expansion of these applications has provided numerous benefits for the users, they also raise concerns about the security and privacy of their biodata, compromising sensitive information such as thoughts, emotions, sexual orientation and religious beliefs [3]. Concepts such as "Neurorights", "Brain Hacking", among others, have emerged to address these issues, and Chile has taken a pioneering step by legislating neurorights protections on 2020 [5]. Without clear regulations and secure design principles, users remain vulnerable to potential manipulation of their neural data.

III. BCI COMMUNICATION PROTOCOLS

Brain-Computer Interface (BCI) devices rely on different communication protocols for data transmission and operational control. Among these protocols, BLE is commonly adopted in BCIs and other IoT devices because of its low power requirements and straightforward integration. However, these same advantages can create vulnerabilities—such as sniffing, spoofing, and Man-in-the-Middle (MitM) attacks—when the encryption and authentication measures in BLE implementations are weak.

For applications that demand higher bandwidth and continuous data throughput, Wi-Fi often proves more suitable, especially in research or clinical environments. Despite its advantages, Wi-Fi remains susceptible to eavesdropping and data interception unless rigid security safeguards are in place. USB and serial ports connections are frequently favored for their speed and reliability, making them an usual option in research-grade and clinical setups to mitigate the risks associated with wireless communication vulnerabilities. However, if proper protocols are not enforced, these wired interfaces can become targets for physical tampering and other attacks. Additionally, some BCIs use ZigBee-based RF communication for low power, long range applications, although interference and limited bandwidth can affect data integrity and reliability.

IV. BCI VULNERABILITIES AND CHALLENGES

Researchers have identified a range of additional cybersecurity threats that jeopardize BCI devices during the complete operational process. This overview spotlights the vulnerabilities found in current literature, particularly for BCIs communicating via BLE, impacting several key phases:

- **Bluetooth Connection.** Devices are susceptible to MitM attacks, data sniffing and spoofing due to weak encryption and authentication in BLE protocols.
- **Signal Acquisition.** Risk to jamming (interference with legitimate signals), spoofing (introduction of fake signals like P300), and replay attacks (reusing recorded signals to simulate inputs).
- **Data Transmission.** Common threats include MitM attacks, cryptographic exploitation and replay attacks.
- **Data Processing.** Susceptible to malware, adversarial attacks, injection attacks, and algorithm manipulation.
- **User Application Interaction.** Vulnerabilities include exploitation through malicious applications, privilege escalation, spoofing, and social engineering, which can lead to unauthorized system control.
- **Neural Cyberattacks.** Susceptible to tampering, injection attacks, overstimulation (neural flooding) and inhibition (neural jamming).

After analyzing and comparing the literature[2-4][7-9], it is evident that BCIs are susceptible to both traditional cybersecurity attacks, such as MitM attacks—where an attacker intercepts the keys exchanged between devices to eavesdrop on communications—and more specialized neural cyberattacks. On the other hand, BCI devices face a multidimensional security challenge, due to a lack of standardization and the absence of Security-by-Design principles. Neither manufacturers nor regulatory bodies have adequately addressed these challenges. After analyzing the vulnerabilities, challenges and existing proposals, our contributions are as follows:

- **Passive Attack Evaluation:** We performed a passive attack on BCIs to evaluate and understand the vulnerabilities they pose. We also conducted additional analyses to comprehend the critical features that impact their level of security.
- **Technical Analysis of Commercial BCIs:** We have performed an analysis of the technical aspects of BCIs

that are currently on the market, to assess their security levels and compare their performance.

- **Security Scoring Framework:** We designed a security scoring framework based on previous work [10] to propose the minimum requirements that a BCI must meet to be categorized as secure.

Recent efforts to secure BCIs such as, blockchain frameworks[2], OS kernel modules[8], and machine learning for threat detection often require high computational resources, add latency, or introduce excessive complexity. Consequently, our work focuses on enhancing the pairing process for a more practical and immediate security improvement.

V. BLUETOOTH LOW-ENERGY PAIRING METHODS

In this section, we present the pairing methods for BLE, introduced in the Bluetooth 4.0 specification. Since its adoption, most devices can support both Bluetooth Classic and BLE (dual mode). This is the most used communication protocol within the commercial BCI devices, due to its two key features; low energy consumption and Generic Attribute Profile (GATT)-based data transmission [11]. Consequently, it is crucial to understand the level of security of each of their pairing methods, to assess and implement a Security-by-Design approach when manufacturing these devices.

The Secure Simple Pairing (SSP) mechanism was developed as a part of the Bluetooth Standard. The main goal of SSP is to establish the link key between two Bluetooth Devices. During this process, SSP uses the Elliptic Curve Diffie-Hellman (ECDH) public key algorithm to protect connections from MitM attacks. SSP offers four different modes of authenticated key exchange, each varying in security depending on the technical design and Input/Output capabilities (IOCaps) [12]:

- **Just Works.** Requires no user interaction and is commonly used when devices lack a display or keyboard, making it the least secure and highly vulnerable to MitM attacks.
- **Numeric Comparison.** Involves verifying a 6-digit code displayed on both devices. While more secure than Just Works, it is often impractical for BCIs, as they don't have screens.
- **Passkey Entry.** Uses a 4- or 6-digit code for authentication. Although more secure with 6 digits, some BCI devices use a default or all-zero passkey, leaving them exposed.
- **Out-of-Band (OOB).** Exchanges keys through an additional channel (e.g., NFC, QR, or wired), significantly reducing the risk of MitM by requiring attackers to compromise both channels simultaneously.

Additionally, the National Institute of Standards and Technology (NIST) recommends that manufacturers implement an Advanced Encryption Standard (AES), as it secures even more the data that is being transmitted [13]. Encryption requires pairing, which performs a key exchange between the master and slave devices. Two key exchange

methods are available under the Secure Connections Only (SCO) mode for BLE devices; Legacy Pairing (BLE 4.0 and 4.1) and Secure Pairing (BLE 4.2+). The main difference is that Legacy Pairing does not include ECDH encryption, which makes it vulnerable to eavesdropping attacks. However, in Bluetooth Classic versions 2.1 and 3.0, SSP is used. This method is less secure than devices that support SCO, emphasizing the need for current commercial devices to adopt the latest encryption and pairing methods, to mitigate risks effectively [11].

VI. PASSIVE ATTACK TEST

In this project, we conducted an experiment as a passive attacker to exploit the vulnerabilities of the Bluetooth protocol during the pairing process of BCI devices. Specifically, we implemented an eavesdropping attack on the exchanged packets. This allows us to verify the current risks that commercial BCI possess for their users. Capturing and recording transmitted packets, MAC addresses and connection parameters, is a critical step that could facilitate more severe attacks, such as MitM.

To execute the sniffing attack, we employed a Nordic Semiconductor Sniffer (nRF52840), to capture the traffic between our BCI devices and a Windows computer. Wireshark was the software that was implemented to capture and analyze the packets that were spotted by our sniffer. All intercepted packets were "LE LL" (Bluetooth Low Energy Link Layer) type, which represents one of the lowest layers of the BLE protocol stack. This layer is responsible for medium access, connection establishment, error control, and flow control [14] (i.e., Advertising and Scanning, Connecting, Data Channels, Encryption). More detailed data from the packets can be identified at the HCI or ATT protocols level. The two BCI devices were tested during the passive attack:

- The NeuroSky MindWave Mobile 2: EEG headset with a static MAC address that uses both Bluetooth Classic and BLE. It features a single EEG channel and employs a 4-digit passkey defaulted to "0".
- OpenBCI Ganglion: 4-channel neural interface for EEG, EMG, and ECG that transmits data via BLE. It also supports a USB dongle for proprietary communication, adding an extra layer of security.

Among the two tested devices, only the MindWave Mobile 2 was identifiable by our sniffer, indicating that a more complex attack could potentially be implemented on this particular device. In contrast, the Open BCI Ganglion device was not detected by our sniffer. This can be attributed to its USB Dongle, which serves as an additional OOB pairing method enhancing security. Additionally, the MindWave Mobile 2's lower price—about one-third that of the Ganglion—suggests that cost-cutting may compromise Security-by-Design practices.

VII. SCORING FRAMEWORK

After running the experimental tests, we reviewed the technical sheets of commercial BCIs to obtain critical and relevant data. Afterwards, based on previous work from article [10], we built a specific framework for BCIs that evaluates six features that were especially selected to build

our scoring system. The evaluation is grounded in industry standards and the best practices for Bluetooth security. The main goal is to mark the minimum requirements manufacturers require to design secure devices and to help mitigate risks such as eavesdropping, MitM attacks, and device tracking. The features that we selected to build the framework were the following:

1. *BLE*. It is an essential protocol for IoT and wearable devices such as BCIs due to its low power consumption and security improvements over Bluetooth Classic. Devices using BLE are awarded 5 points, as they meet modern standards for secure communication. Devices without BLE receive only 1 point.
2. *Secure Connections*. By using authenticated pairing and Elliptic Curve Diffie Hellman (ECDH) key exchange, the Bluetooth Secure Connections protocol significantly strengthens defenses against threats such as MitM attacks. BCI devices using LE Secure Connections earn 3 points. LE Legacy Pairing receives 2 points, and Simple Pairing only 1 point.
3. *Just Works Association Model*. This pairing method lacks user authentication, making it insecure. Devices that avoid Just Works receive 2 points, while those that rely on it receive 1 point.
4. *Passkey Requirement*. This method adds a layer of user authentication. A 6-digit passkey raises the total combinations from 10,000 to 1,000,000, making it far more secure than a 4-digit passkey. Consequently, 6-digit passkey devices earn 5 points, 4-digit passkey devices get 2 points, and those without any passkey functionality only 1 point.
5. *OOB Pairing*. This is one of the most secure association models, OOB relies on an additional communication channel (e.g., USB dongle, NFC, QR) for key exchange. Devices with OOB pairing receive 3 points, while those lacking this feature receive 1 point.
6. *Non-Static Address*. Although not commonly used in BCIs, it is already prevalent in other IoT devices. Randomizing addresses complicates tracking by attackers. BCIs implementing non-static addresses earn 2 points; those using static addresses receive 1 point.

After evaluating these six features across seven commercial BCI devices, we did a comparison on Table I, that illustrates how each device aligns with current Bluetooth security requirements. From these findings, we developed a scoring framework explained on Figure 6, that sets 14 points out of 20 as the minimum threshold for a BCI to be considered secure. Features such as BLE pairing and Secure Connections are crucial due to their role in mitigating cyberattacks, while OOB pairing is also emphasized as a key factor for higher security.

Among the seven evaluated BCI devices that are shown on Figure 1, only two of them surpassed the proposed minimum requirements. The *Emotiv Epoc X* emerged as the most secure, achieving the highest score of 15 points, thanks to its robust implementation of LE Secure Connections and

OOB pairing. Similarly, the *OpenBCI Ganglion*, which we used during the passive attack experiment, met the minimum security threshold, making it a reliable option for customers. In contrast, devices like the *NeuroSky MindWave 2*, *Muse 2*, and *BrainCo FocusCalm* fell just below the threshold due to their reliance on less secure pairing mechanisms, and the absence of OOB pairing. The least secure device was the *Bitbrain Hero*, which lacked essential security features entirely.

TABLE I. COMMERCIAL BCI'S BLUETOOTH FEATURES

Device Name	BL ^a	SC ^b	BLE	JW ^c	PK ^d	OOB	NSA ^e
OpenBCI Ganglion	4.0	LE Legacy Pairing	✓	X	X	✓	X
NeuroSky MindWave Mobile 2	2.1	Secure Simple Pairing	✓	X	4-dig	X	X
Emotiv Epoc X	5.0	LE Secure Connections	✓	X	X	✓	X
Muse 2	4.2	LE Secure Connections	✓	✓	X	X	X
Neurable (MW75)	5.2	LE Secure Connections	✓	✓	X	X	X
BrainCo FocusCalm	5.0	LE Secure Connections	✓	✓	X	X	X
Bitbrain Hero	2.1	Secure Simple Pairing	X	✓	X	X	X

^a Bluetooth Protocol.

^b Secure Connection.

^c Just Works.

^d Passkey Entry.

^e Non-Static Address.

REFERENCES

- [1] J. Van Erp, F. Lotte, and M. Tangermann, "Brain-Computer Interfaces: Beyond Medical Applications," *Computer*, vol. 45, no. 4, pp. 26–34, Apr. 2012, doi: 10.1109/MC.2012.107.
- [2] A. A. Khan, A. A. Laghari, A. A. Shaikh, M. A. Dootio, V. V. Estrela, and R. T. Lopes, "A blockchain security module for brain-computer interface (BCI) with Multimedia Life Cycle Framework (MLCF)," *Neuroscience Informatics*, vol. 2, no. 1, p. 100030, Mar. 2022, doi: 10.1016/j.neuri.2021.100030.
- [3] S. L. Bernal, A. H. Celdrán, G. M. Pérez, M. T. Barros, and S. Balasubramaniam, "Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges," *ACM Comput. Surv.*, vol. 54, no. 1, pp. 1–35, Jan. 2022, doi: 10.1145/3427376.
- [4] S. N. Abdulkader, A. Atia, and M.-S. M. Mostafa, "Brain computer interfacing: Applications and challenges," *Egyptian Informatics Journal*, vol. 16, no. 2, pp. 213–230, Jul. 2015, doi: 10.1016/j.eij.2015.06.002.
- [5] A. Zúñiga-Fajuri, L. Villavicencio Miranda, D. Zaror Miralles, and R. Salas Venegas, "Chapter Seven - Neurorights in Chile: Between neuroscience and legal science," pp. 165–179, 2021, doi: 10.1016/bs.dnb.2021.06.001.
- [6] S. L. Bernal, A. H. Celdrán, and G. M. Pérez, "Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity," *Commun. ACM*, vol. 66, no. 4, pp. 68–78, Apr. 2023, doi: 10.1145/3535509.
- [7] O. Landau, R. Puzis, and N. Nissim, "Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space," *ACM*

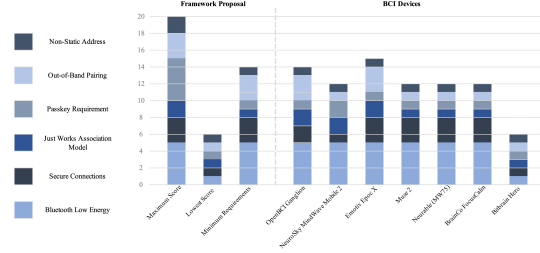


Fig. 1. Scoring Framework applied on BCI devices.

VIII. CONCLUSIONS AND FINAL THOUGHTS

The popularity and adoption of BCI devices are increasing in diverse domains, from healthcare and research to daily activities. However, our state-of-the-art analysis and our passive attack experiment, unveiled critical vulnerabilities and challenges in current BCI devices. The lack of standardization and Security-by-Design is largely overlooked by manufacturers and regulators. This issue poses significant risks to the confidentiality of users' neuro data, especially as these devices become more widely accessible. By proposing a scoring framework based on actual Bluetooth security standards, we aim to encourage manufacturers, researchers, and regulators to adopt a Security-by-Design approach when developing these devices, before releasing them on the market. However, we assessed the safety levels of seven commercial BCI devices using our proposed framework, and only two surpassed the minimum security threshold. This outcome highlights the current lack of focus on safeguarding users' neural data during the production of BCI devices. Finally, our ultimate goal is to ensure and safeguard the integrity of users, positioning BCIs as a secure technology for future developments.

- [8] Z. Tarkhani, L. Qendro, M. O. Brown, O. Hill, C. Mascolo, and A. Madhavapeddy, "Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces," Jan. 19, 2022, arXiv: arXiv:2201.07711, doi: 10.48550/arXiv.2201.07711.
- [9] A. N. Belkacem, "Cybersecurity Framework for P300-based Brain Computer Interface," in *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Toronto, ON, Canada: IEEE, Oct. 2020, pp. 1–6, doi: 10.1109/SMC42975.2020.9283100.
- [10] A. G. Silva-Trujillo, M. J. González González, L. P. Rocha Pérez, and L. J. García Villalba, "Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack," *Sensors*, vol. 23, no. 12, p. 5438, Jun. 2023, doi: 10.3390/s23125438.
- [11] Y. Zhang, "Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks".
- [12] Y. Haotian, "Security analysis of Bluetooth Secure Simple Pairing protocols with extended threat model," vol. 72, Feb. 2023, doi: https://doi.org/10.1016/j.jisa.2022.103385.
- [13] D.-Z. Sun, Y. Mu, and W. Susilo, "Man-in-the-middle attacks on Secure Simple Pairing in Bluetooth standard V5.0 and its countermeasure," *Pers Ubiquit Comput*, vol. 22, no. 1, pp. 55–67, Feb. 2018, doi: 10.1007/s00779-017-1081-6.
- [14] M. Siekkinen, M. Hienkari, J. K. Nurminen, and J. Nieminen, "How low energy is bluetooth low energy? Comparative measurements with ZigBee/802.15.4," in *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Paris, France: IEEE, Apr. 2012, pp. 232–237, doi: 10.1109/WCNCW.2012.6215496.

Chapter 2

Presentation

This chapter contains the slides presented at the URSI conference in Tarragona and the previous exam. The presentation was elaborated in english format to accord the paper with the information provided during the presentation and to fullfill the requirements of international conferences.



Cyberattacks Study and Privacy in Brain-Computer Interfacing Devices

Antonio de Jesús Menchaca-Martínez^{*,+}, Alejandra Guadalupe Silva-Trujillo⁺,
Pedro David Arjona- Villicaña⁺

(^{*}) Collège STEE, Université de Pau et des Pays de l'Adour (UPPA), Anglet, France

(⁺) Facultad de Ingeniería, Universidad Autónoma de San Luis Potosí (UASLP), San Luis Potosí, Mexico

September
2025



Overview

01	Introduction & Background	12	Research Questions
02	Applications	13	Objectives
03	BCI Technology	14	Methology
05	BCI Communication Protocols	15	Passive Attack
09	BCI Vulnerabilities and Challenges	19	Scoring Framework
10	Security Concerns	23	Conclusions



Introduction & Background

- **What are BCIs?** Brain-Computer Interfaces (BCIs) are neurotechnologies that enable direct communication between the brain and computers, bypassing traditional input methods.
- **How do they work?** They capture neural signals to control devices (e.g., robotic arms) or restore motor function, without relying on muscular or speech input.
- **Importance:** With BCIs increasingly used in both medical and non-medical applications, ensuring the security and privacy of sensitive neural data has become critical.
- **Problem Statement:** Cybersecurity gaps in current BCI implementations, compromising neural data and user privacy.

NeuroSky[®]
Body and Mind. Quantified.

OPENBCI

synchron

NEURALINK



01

Applications



Neuroergonomics and
Smart Environments



Neuromarketing and
Advertisement



Education and
Self-Regulation



Games and
Entertainment



Security and
Authentication



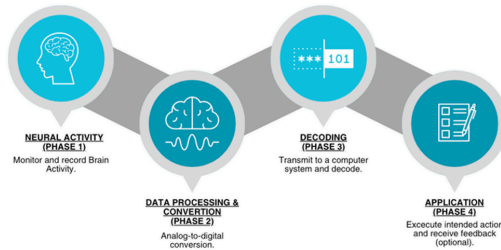
Healthcare

02

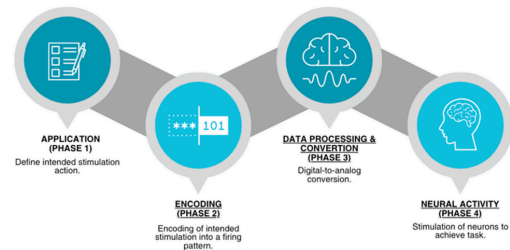
State of the Art

BCI Technology

Neural Data Acquisition

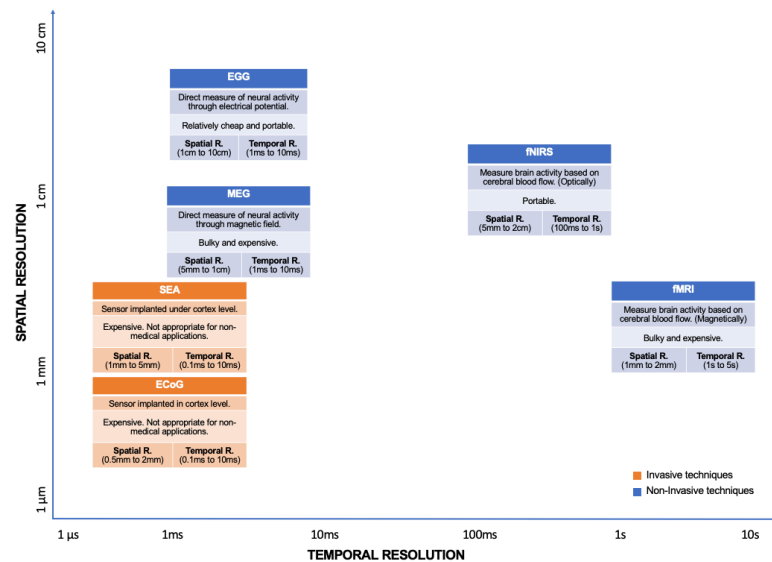


Neural Stimulation



03

BCI Technology



04

BCI Communication Protocols

Device Name	Channels	Signal Type	Supported Protocols	Applications
OpenBCI Ganglion	4	EEG, EMG, ECG	Bluetooth LE, USB, ZigBee (custom)	Research, neurofeedback
NeuroSky MindWave Mobile 2	1	EEG	Bluetooth LE, Bluetooth 4.0, ZigBee (custom)	Education, gaming, personal
Emotiv Epoc+	14	EEG	Classic Bluetooth, USB dongle	Research, gaming, neuromarketing
Muse 2	7	EEG	Bluetooth LE	Meditation, mindfulness
g.tec g.USBamp	16 to 256	EEG, EMG, ECG	USB, ZigBee (custom)	Clinical diagnostics, research
Neurable (MW75)	6	EEG	Bluetooth LE, USB, ZigBee (custom)	AR/VR control, gaming
NextMind	1	EEG	Bluetooth LE	AR/VR, hands-free control
BrainCo FocusCalm	4	EEG	Bluetooth LE	Education, cognitive training
Kernel Flow 2	Multiple	NIRS	Wi-Fi, Bluetooth LE	Cognitive research, clinical
Bitbrain Diadem	8 to 32	EEG	Wi-Fi, Bluetooth LE, USB, ZigBee (custom)	Research, clinical use

05

Bluetooth Low-Energy (BLE)

Pairing Modes:

- **Just Works:**
 - Pairs without user interaction.
 - Limitation: Vulnerable to MITM attacks (common in devices lacking displays).
- **Numeric Comparison:**
 - Both devices display a 6-digit number; user confirms if they match.
 - Limitation: Not practical for many BCIs without screens.
- **Passkey Entry:**
 - One device generates a passkey (4 or 6 digits) that must be manually entered.
 - Best Practice: 6-digit passkeys offer significantly better security than 4-digit ones.
- **Out-of-Band (OOB):**
 - Uses an alternative secure channel (e.g., NFC, QR code, wired connection) to exchange the key.
 - Advantage: Minimizes MITM risks by requiring compromise of both channels.

06

Security Concerns

Cyberattack Threats:

- **Sniffing & Spoofing:** Attackers can intercept and mimic neural data, potentially leading to unauthorized control or data manipulation.
- **Man-in-the-Middle (MITM) Attacks:** Vulnerabilities, especially in BLE protocols, allow adversaries to intercept and alter communication during pairing and data transmission.

Design & Standardization Gaps:

- **Fragmented Cybersecurity Measures:** Many BCIs lack a unified, robust security framework.
- **Absence of Security-by-Design:** Security is often an afterthought, leaving critical vulnerabilities unaddressed from the start.

07

Security Concerns

Ethical & Legal Implications:

- **Neuro Rights at Risk:** Inadequate protection of neural data threatens fundamental rights to mental privacy and cognitive integrity.
- **Data Privacy Concerns:** Unauthorized access to biometric and neural data could have severe personal and legal consequences.

Urgency & Impact:

- As BCIs become integrated into healthcare, consumer tech, and everyday applications, these vulnerabilities pose significant risks to user safety, privacy, and overall trust in neurotechnology.

08

Research Questions

- What are the main security vulnerabilities in current brain-computer interfaces?
- How can cyberattacks affect the privacy and security of BCI users?
- What security framework can be developed to mitigate risks associated with BCI devices across various application environments?
- What is the impact of existing legal and ethical frameworks on data privacy protection in BCIs, and what improvements are needed?
- How can privacy-by-design techniques be integrated into the development of new BCI systems to ensure security from the start?

10



Objectives

- Identify common cyberattacks on BCIs.
- Analyze vulnerabilities during the BCI process and evaluating the impact on users' privacy and the latent risks to user safety.
- Compare different BCI devices security properties and vulnerabilities, and classify their risk.
- Propose a comprehensive framework for enhancing BCI security and user privacy protections, and provide minimum design requirements.

Methodology

1. Literature Review

- Identify current BCI technologies.
- Assess known vulnerabilities.

2. Analyze Cyberattacks Patterns

- Study common and emerging threats.
- Correlate threats with BCI vulnerabilities.

3. Conduct Tests

- Test BCI responses to sniffing.
- Identify weaknesses in BCI security.

4. Propose Countermeasures

- Design security enhancements.
- Recommend implementation strategies.

11

Passive Attack

Experiment Overview

Goal of Experiment

- Demonstrate how a passive attacker can capture Bluetooth packets during the BCI pairing process.

Methodology

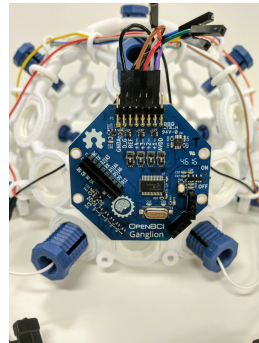
- Devices Tested:
 - NeuroSky MindWave Mobile 2 (EEG)
 - OpenBCI Ganglion (EEG/EMG/ECG)
- Tools Used:
 - Nordic Semiconductor Sniffer (nRF52840)
 - Wireshark for packet capture and analysis

Why This Matters

- Exposing how easily packets can be intercepted underscores the need for stronger pairing methods and robust encryption.

12

Passive Attack



OpenBCI Ganglion
Cost: 500 EUR



Neurosky Mindwave Mobile 2
Cost: 150 EUR

13

Passive Attack

prueba1 pcapng

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

Interface Device All advertising devices Key Legacy Paskey Value Adv Hop Help Defaults Log

No.	Time	Source	PHY	Protocol	Length	Delta time (s) end to start	SN	NESN	More Data	Event counter	Info
1776	25.047	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
1830	25.076	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
1845	25.782	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
1940	26.939	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
1952	26.941	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
1966	27.153	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
1973	27.252	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2011	27.669	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2131	29.061	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2153	29.274	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2224	30.005	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2246	30.224	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2320	31.083	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2363	31.612	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2394	31.930	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2426	32.245	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2437	32.348	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2483	32.866	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2486	32.867	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2501	32.972	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2505	33.071	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2540	33.381	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2556	33.594	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP
2559	33.596	TexasInstrument_e8:50:99	LE	IM	23	151µs				0	SCAN_RSP
2610	34.440	TexasInstrument_e8:50:99	LE	IM	23	150µs				0	SCAN_RSP

> Frame 1776: 49 bytes on wire (392 bits), 49 bytes captured (392 bits) on interface 0
 > nRF Sniffer for Bluetooth LE
 > Bluetooth Low Energy Link Layer

0000 07 2a 00 03 68 07 02 0a 01 27 2c 00 00 2d 68 24
 0010 04 d6 be 80 8e 04 17 99 50 e8 e3 64 c4 10 09 4d
 0020 69 6e 64 57 61 76 65 20 4d 6f 62 69 6c 65 92 ac
 0030 fd

prueba1 pcapng Packets: 20313 Displayed: 669 (3.3%) Profile: Profile_nRF_Sniffer_Bluetooth_LE

Wireshark

14

Attack Details & Observations

Captured Data:

- "LE LL" packets at the Bluetooth Low Energy Link Layer
- MAC addresses, connection parameters, partial device identifiers

Key Findings

- **MindWave Mobile 2** was detectable by the sniffer, revealing its static MAC address and 4-digit passkey set to "0000."
- **OpenBCI Ganglion** was not detected, thanks to its proprietary USB dongle (an **Out-of-Band pairing method**).

Implications

- Lower-cost devices often lack robust Security-by-Design, making them vulnerable to more complex attacks like MITM.
- OOB pairing significantly reduces susceptibility to passive sniffing.

15

<i>Criterion</i>	<i>Scoring System</i>	<i>Notes</i>
Bluetooth Low Energy (BLE)	Uses BLE: 5 points No BLE: 1 point	BLE is essential for low power consumption and improved security over Bluetooth Classic.
Secure Connections	LE Secure Connections: 3 points LE Legacy Pairing: 2 points Simple Pairing: 1 point	LE Secure uses authenticated pairing with ECDH, providing stronger defense against MITM attacks.
Just Works Model	Avoided: 2 points Used: 1 point	"Just Works" lacks authentication, so its use lowers security.
Passkey Requirement	6-digit passkey: 5 points 4-digit passkey: 2 points No passkey: 1 point	More digits greatly enhance the security of the pairing process.
Out-of-Band (OOB) Pairing	OOB supported: 3 points Not supported: 1 point	OOB pairing adds an extra secure channel for data exchange, reducing the risk of attacks.
Non-Static Address	Non-static: 2 points Static: 1 point	Randomized addresses help prevent device tracking and enhance overall security.

Maximum score: 20 points

Minimum requirements: 14 points

16

Scoring Framework

TABLE IV. COMMERCIAL BCI'S BLUETOOTH FEATURES

<i>Device Name</i>	<i>BL</i> ^b	<i>SC</i> ^c	<i>BLE</i>	<i>JW</i> ^d	<i>PK</i> ^e	<i>OOB</i>	<i>NSA</i> ^f
OpenBCI Ganglion	4.0	LE Legacy Pairing	✓	X	X	✓	X
NeuroSky MindWave Mobile 2	2.1	Secure Simple Pairing	✓	X	4-dig	X	X
Emotiv Epoc X	5.0	LE Secure Connections	✓	X	X	✓	X
Muse 2	4.2	LE Secure Connections	✓	✓	X	X	X
Neurable (MW75)	5.2	LE Secure Connections	✓	✓	X	X	X
BrainCo FocusCalm	5.0	LE Secure Connections	✓	✓	X	X	X
Bitbrain Hero	2.1	Secure Simple Pairing	X	✓	X	X	X

^a Bluetooth Protocol.

^b Secure Connection.

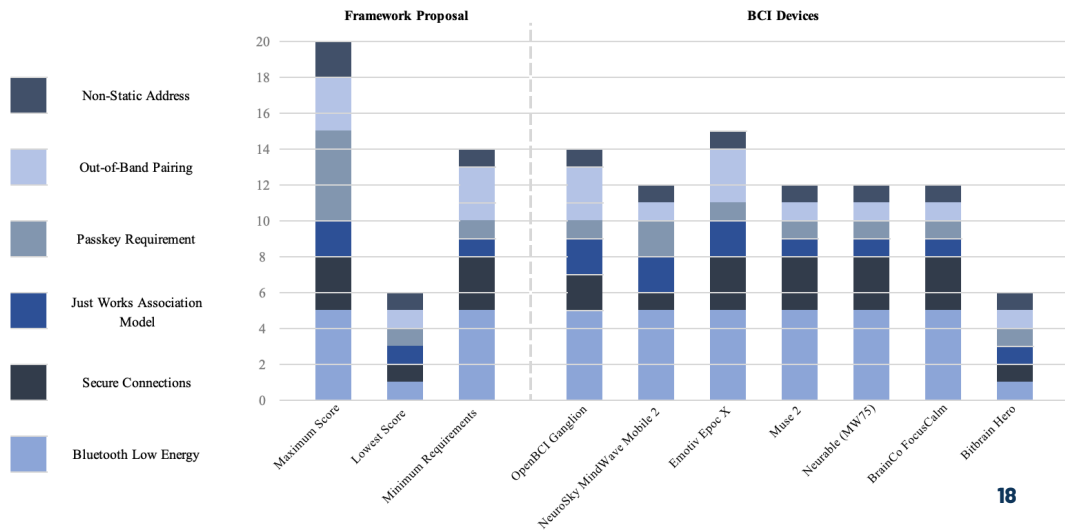
^c Just Works.

^d Passkey Entry.

^e Non-Static Address.

17

Scoring Framework



18

TABLE III. EXISTING SOLUTIONS AND OUR APPROACH

<i>Security Approach</i>	<i>What They Do/Offer</i>	<i>Limitations/Focus</i>
Blockchain Frameworks [2]	Use decentralization, immutability, and smart contracts to secure communications.	High computational overhead and increased latency make them unsuitable for real-time BCI applications.
OS Kernel Modules & User-Space Frameworks [11]	Harden system level defenses and mitigate vulnerabilities.	Introduce complexity and require specialized expertise, which can be impractical for many BCI systems.
Machine Learning for Threat Detection [8]	Provide proactive security by identifying potential attacks.	Current BCI and IoT devices lack the robust computational power necessary for efficient real-time processing.
Our Approach: Enhancing the Pairing Process	Targets the pairing phase, a critical vulnerability in BCI communications.	Offers a practical, low-overhead security enhancement that aligns with the real-time requirements of current BCI devices.

19

Summary of Findings

- **Rapid BCI Adoption:** BCIs are increasingly used in healthcare, research, and daily life.
- **Identified Vulnerabilities:** State-of-the-art review and passive attack tests revealed critical security gaps, especially in devices lacking robust pairing methods.
- **Scoring Framework Results:** Of seven commercial devices evaluated, only two surpassed the minimum security threshold, highlighting a widespread lack of Security-by-Design.

20

Key Recommendations

- **Adopt Security-by-Design:** Manufacturers should integrate cybersecurity measures (e.g., OOB pairing, non-static addresses) from the initial design phase.
- **Regulatory Guidance:** Policymakers need to establish clear standards and guidelines for BCI security, ensuring user data protection.
- **Future Research Directions:**
 - Develop advanced encryption and low-latency security methods suited for real-time BCIs.

21

Thanks for your attention!

¡Gracias por su atención!

Merci pour votre attention!

23

International Recognition of Our Research

Conference Presentation:

- “Cyberattacks Study and Framework in Brain-Computer Interfacing Devices”
- Presented at the **XL Simposio Nacional URSI 2025 (Unión Científica Internacional de Radio)**
- Tarragona, Spain – September 3–5, 2025
- Accepted and Presented in the **Special Session on 5G/6G & Emerging Technologies**

Publication Opportunity:

- Article submitted for publication in **Computers (MDPI, Open Access Journal)**
- <https://www.mdpi.com/journal/computers>



22

References

- [1] Jan B.F. van Erp, Fabien Lotte, Michael Tangermann. Brain-Computer Interfaces: Beyond Medical Applications. *Computer*, 2012, 45 (4), pp.26-34. ff10.1109/MC.2012.107ff. fffhal-00688344
- [2] Bernal, S. L., Celdrán, A. H., Pérez, G. M., Barros, M. T., & Balasubramaniam, S. (2019). Cybersecurity in Brain-Computer Interfaces: State-of-the-art, opportunities, and future challenges. *arXiv preprint arXiv:1908.03536*.
- [3] Jan B.F. van Erp, Fabien Lotte, Michael Tangermann. Brain-Computer Interfaces: Beyond Medical Applications. *Computer*, 2012, 45 (4), pp.26-34. ff10.1109/MC.2012.107ff. fffhal-00688344
- [4] Abdulkader, S. N., Atia, A., & Mostafa, M. S. M. (2015). Brain computer interfacing: Applications and challenges. *Egyptian Informatics Journal*, 16(2), 213-230.
- [5] Bernal, S. L., Celdrán, A. H., Pérez, G. M., Barros, M. T., & Balasubramaniam, S. (2021). Security in brain-computer interfaces: state-of-the-art, opportunities, and future challenges. *ACM Computing Surveys (CSUR)*, 54(1), 1-35.
- [6] Zúñiga-Fajuri, A., Miranda, L. V., Miralles, D. Z., & Venegas, R. S. (2021). Neurorights in Chile: Between neuroscience and legal science. *Developments in neuroethics and bioethics*, 4, 165-179.
- [7] Martinovic, I., Davies, D., Frank, M., Perito, D., Ros, T., & Song, D. (2012). On the Feasibility of {Side-Channel} Attacks with {Brain-Computer} Interfaces. In 21st USENIX Security Symposium (USENIX Security 12) (pp. 143-158).
- [8] Bernal, S. L., Celdrán, A. H., & Pérez, G. M. (2021). Eight reasons why cybersecurity on novel generations of brain-computer interfaces must be prioritized. *arXiv preprint arXiv:2106.04968*.
- [9] Khan, A. A., Laghari, A. A., Shaikh, A. A., Dootio, M. A., Estrela, V. V., & Lopes, R. T. (2022). A blockchain security module for brain-computer interface (BCI) with multimedia life cycle framework (MLCF). *Neuroscience Informatics*, 2(1), 100030.
- [10] Landau, O., Puzis, R., & Nissim, N. (2020). Mind your mind: EEG-based brain-computer interfaces and their security in cyber space. *ACM Computing Surveys (CSUR)*, 53(1), 1-38.

Appendix A

As the article presented at the conference had to be shortened to comply with the established guidelines, this chapter presents the extended version, which includes additional details about the research project and is intended for future publication using the MDPI format.

Article

Cyberattacks Study and Privacy in Brain-Computer Interfacing Devices

Antonio de Jesús Menchaca-Martínez ¹ , Alejandra Guadalupe Silva-Trujillo ^{2*} and Pedro David Arjona-Villicaña ²¹ Collège STEE, Université de Pau et des Pays de l'Adour (UPPA), Anglet, France; adjmmartinez@univ-pau.fr² Facultad de Ingeniería, Universidad Autónoma de San Luis Potosí (UASLP), San Luis Potosí, México; asilva@uaslp.mx; david.arjona@uaslp.mx

* Correspondence: asilva@uaslp.mx

Abstract: Advanced neurotechnologies, particularly Brain-Computer Interfaces (BCIs), are revolutionizing human-machine interactions, providing remarkable advancements across medical, industrial, educational, entertainment, and security domains. Despite BCIs' great potential, they simultaneously raise critical ethical concerns regarding user data privacy and their Neuro Rights, which aim to safeguard individuals against the risks of emerging neurotechnologies, especially as they become increasingly available on the market. Utilizing a comprehensive literature review and implementing a passive attack on two commercial BCI devices, the study reveals critical vulnerabilities during all the phases of the system. Our findings underscore the urgent need for robust cybersecurity frameworks, including Privacy-by-Design strategies. To address this problem, we designed a scoring framework based on the Bluetooth standard, that guides manufacturers and helps regulators, guaranteeing the safe adoption of BCIs. The proposed solution aims to enhance the security of the pairing process on BCI devices, thereby ensuring user neural data integrity and protection.

Keywords: Neurorights; BCIs; cybersecurity; neural data privacy; BLE

1. Introduction

Brain-Computer Interfaces (BCIs) are a neurotechnology that enables communication and control between users and computer systems beyond traditional keyboard-based interaction. They do not rely on any other external devices nor human intervention (i.e., muscular or speech) to complete an intended task, such as controlling a robotic arm or restoring motor function in individuals with spinal cord injuries [1]. Furthermore, BCIs can also provide a real-time communication between the brain and external digital devices through brain-to-internet (B2I) connectivity [2]. With the adoption of 6G technology, that promises ultra-low latency and massive connectivity, the integration of BCIs into everyday applications is expected to accelerate, requiring a reassessment of cybersecurity frameworks to protect increasingly interconnected neural devices.

The feedback loop of BCIs is defined by its directionality, which not only depends on the user's intended goals, but also on the device's design and the context it is being used. In one direction we have the "Neural Data Acquisition" process (Figure 1), where BCIs monitor and records brain activity (Phase 1). These neural signals reflect the user's intentions to control an external device or interface. The raw neural signals generated by the brain then undergo conversion and processing (Phase 2), including analog-to-digital transformations that aim to optimize the Signal-to-Noise Ratio. Next, the digital neural data is transmitted to a computer system (Phase 3), where algorithms such as classifiers or

Received:

Revised:

Accepted:

Published:

Citation: Menchaca-Martínez, A. de J.; Silva-Trujillo, A. G.; Arjona-Villicaña, P. D. Cyberattacks Study and Privacy in Brain-Computer Interfacing Devices. *Journal Not Specified* **2025**, *1*, 0. <https://doi.org/>

Copyright: © 2025 by the authors. Submitted to *Journal Not Specified* for possible open access publication under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

predictors decode them to infer the user’s contemplated action. Ultimately, the interpreted command triggers the corresponding application behavior, closing out the cycle (Phase 4) and often activating additional feedback loops for further refinement [3].

Neural Data Acquisition

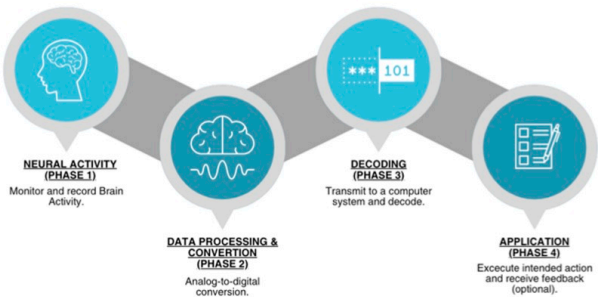


Figure 1. Neural Data Acquisition Cycle.

Neural Stimulation

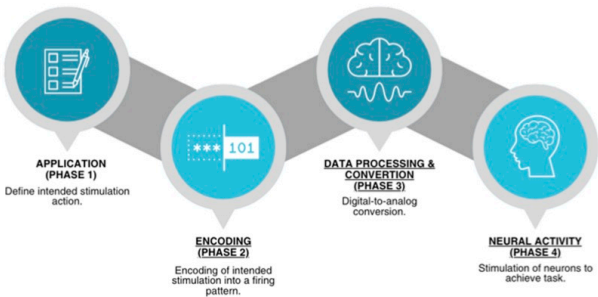


Figure 2. Neural Stimulation Cycle.

In the other direction “Neural Stimulation” (Figure 2), the BCI delivers brain stimulation, through transcranial magnetic stimulation (TMS) or electrical pulses, to modulate neural activity (e.g., employing TMS to target specific brain regions associated with cognitive decline in Alzheimer’s patients). This cycle begins with applications defining the intended stimulation task to perform (Phase 1). This input is then processed by different techniques, such as Machine Learning (ML) models to develop a firing pattern containing all the necessary parameters for brain stimulation, including pulse width, intensity, frequency and temporal planning (Phase 2). Subsequently, the BCI converts these digital parameters into analog data and transmits it to the stimulation system (Phase 3). Finally, this system will stimulate specific neurons from one or more brain regions to achieve the desired outcome (Phase 4) [3].

BCIs can be designed to function either unidirectionally or bidirectionally, depending on whether they simply collect neural signals or both collect and stimulate them. In a unidirectional BCI, the communication system implies that either acquisition of neural

data or neural stimulation is performed, making it simpler to design and implement. However, this simplicity also limits its range of applications. By contrast, bidirectional BCIs can both acquire neural data and stimulate neurons, allowing for a more interactive and sophisticated exchange between the brain and the external device. Although this expanded capability can power an array of advanced applications, the added complexity typically translates to higher development costs.

Brain activity can be measured using different hardware technologies, which can be classified into invasive and non-invasive techniques. Non-invasive techniques include Electroencephalography (EEG), Magnetoencephalography (MEG), functional Magnetic Resonance Imaging (fMRI), and functional Near-Infrared Spectroscopy (fNIRS). Invasive techniques comprise Electrocorticography (ECoG) and Subcortical Electrode Arrays (SEA). The authors Landau et al. in article [4] provide detailed descriptions of these BCI hardware technologies, and our synthesis and categorization of these technologies are presented in Figure 3 for comprehensive reference. Notably, the majority of BCIs rely on EEG technology to record the electrical fields generated by neuronal synaptic activity. According to their frequency, there are specific bands classified as delta (δ , 1–4 Hz), theta (θ , 4–7 Hz), alpha (α , 8–13 Hz), beta (β , 13–30 Hz), and gamma (γ , >30 Hz)[5]. These signals are collected from scalp electrodes, and amplified to enhance the Signal-to-Noise Ratio and continuously sampled at a high frequency (typically ranging from 128 Hz to 512 Hz) to provide a precise temporal resolution [6], making EEG an ideal method with a simple set up. Moreover, its portability and affordability allow users to independently operate EEG devices, increasing its popularity and the need to secure these devices against cyberattacks compared to other brainwave acquisition methods.

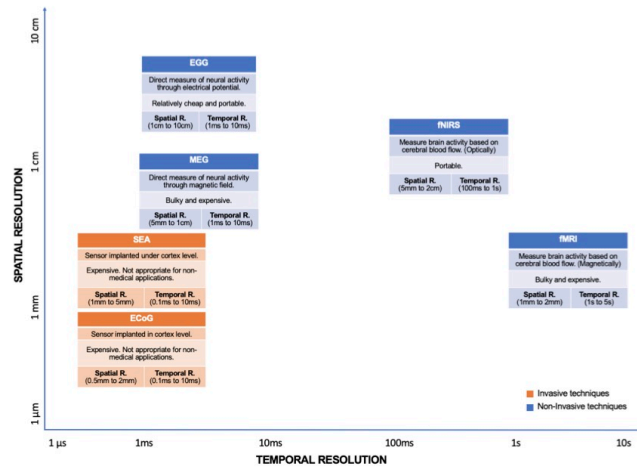


Figure 3. BCIs hardware technologies comparison.

This paper focuses on the vulnerabilities that BCIs face during the pairing process, as most of them use the Bluetooth protocol to communicate with an external device. Section 2 provides a solid background on the evolution of BCI devices, their expansion into several fields and the issues regarding user privacy. In Section 3, we identify the communication protocols used by current devices that are on the market, identifying the common pairing method and shared vulnerabilities. In Section 4, we implement a systematic review of current vulnerabilities and challenges found on the state-of-the-art literature, which guided us through to propose a novel solution. After identifying the existing lack of security

by design and standardization for these devices on several studies, Section 5 explains how the Bluetooth Low Energy protocol works and outlines its different pairing methods. In Section 6, we performed a passive attack on two BCI devices, to demonstrate from a practical perspective, some of the vulnerabilities those devices might face during a cyberattack. Section 7 presents our proposed scoring framework for minimum security requirements, which we used to evaluate current devices that are on the market. Finally, in Section 8 we present our conclusions about our findings and proposal.

2. BCI Applications and User Privacy

Since its origins in the 1970's, Brain-Computer Interfaces (BCIs) and brain monitoring have primarily served medical applications in healthcare [3]. Initially, BCIs were developed to assist individuals with severe disabilities, enabling them to communicate and control their environment through direct brain signals. Over the decades, the technology has significantly evolved, finding applications not only in medical diagnostics and treatment but also in preventive care, rehabilitation, and restoration of lost functions. These advancements are comprehensively detailed by authors Abdulkader et al. in article [7], and we outlined them in Table 1, to highlight the diverse roles BCIs play in enhancing patient care and medical outcomes.

Table 1. Medical scopes and functionalities of BCIs.

Medical Scope	BCI Applications and Functionalities
Prevention	- Studies measure the influence of smoking and alcohol on brainwaves to assess potential loss of function and decreased alertness. - Motion sickness prediction systems help prevent traffic accidents by monitoring driver alertness and consciousness through BCI-based systems.
Detection & Diagnosis	- EEGs are utilized for brain tumor detection as a more cost-effective alternative to MRI and CT scans. - BCI systems assist in detecting health issues such as epilepsy, narcolepsy, and dyslexia. - EEG signals can help predict diseases like Parkinson's, dyskinesia, peripheral neuropathy, and musculoskeletal disorders.
Rehabilitation & Restoration	- BCIs aid in restoring lost functions and improving mobility in patients with strokes, injuries, and disabilities. - BCI-based prosthetic limbs assist patients in regaining functionality. - Rehabilitation training programs using real-world tasks, virtual reality, and augmented reality. - Motor imagery signals are used in neurofeedback systems for post-stroke motor therapy.

As research and technology continue to advance, BCIs have expanded their scope into diverse non-medical fields. These applications include Neuroergonomics and Smart Environments, such as smart houses, workplaces, and transportation systems; Neuromarketing and Advertisement, involving Electroencephalogram (EEG) evaluations for advertisements in both commercial and political contexts; Educational and Self-Regulation settings, en-

abling and enhancing skill learning through techniques like functional Magnetic Resonance Imaging (fMRI) neurofeedback; Games and Entertainment, covering from brain-controlling games to Virtual Reality; and Security and Authentication, where methods like Cognitive Biometrics and Electrophysiology using biosignals enhance authentication processes [7].

While the expansion of these applications has provided numerous benefits for the users, they also raise concerns about the security and privacy of their biodata, compromising sensitive information such as thoughts, emotions, sexual orientation and religious beliefs [3]. The potential threat of a cyberattack leaves users vulnerable, highlighting the need for robust security measures in the rapidly evolving landscape of BCI applications. Protecting users from these potential dangers has become a concern in the field of cybersecurity. This has given rise to concepts such as “Neuro Rights,” “Neuro Security,” “Neuro Privacy,” “Neuro Ethics,” “Neuro Confidentiality,” “Neuro Integrity,” “Brain Hacking” among others, all aimed at ensuring that users are considered and protected amidst the ongoing technological revolution. Chile stands as a pioneer in the Americas by introducing two bills in its congress in 2020 aimed at preserving Neuro Rights and safeguarding the mental integrity of users. These legislative initiatives also seek to regulate the development, research, and advancement of neurotechnologies [8].

Despite the growing market of BCIs and other IoT devices, there is a lack of cybersecurity standards focusing on Security-by-Design and Privacy-by-Design principles. This gap underscores the urgency of implementing protective frameworks, and a call to action on both manufacturers and regulators. Moreover, invasive BCIs present an even greater challenge, as demonstrated by new technologies like Neuralink, which recently implanted its first device in a human subject. Neuralink uses a communication protocol based on Bluetooth and a nanotechnology for single-neuron precision. If there is no regulation or standardization implemented while designing these devices, users are vulnerable to malicious manipulation of their neural activity by attackers [9].

3. BCI Communication Protocols

Brain-Computer Interface (BCI) devices rely on different communication protocols for data transmission and operational control. Among these protocols, Bluetooth Low Energy (BLE) is commonly adopted in BCIs and other IoT devices because of its low power requirements and straightforward integration. However, these same advantages can create vulnerabilities—such as sniffing, spoofing, and man-in-the-middle attacks—when the encryption and authentication measures in BLE implementations are weak.

For applications that demand higher bandwidth and continuous data throughput, Wi-Fi often proves more suitable, especially in research or clinical environments. Despite its advantages, Wi-Fi remains susceptible to eavesdropping and data interception unless rigid security safeguards are in place. USB and serial ports connections are frequently favored for their speed and reliability, making them an usual option in research-grade and clinical setups to mitigate the risks associated with wireless communication vulnerabilities. However, if proper protocols are not enforced, these wired interfaces can become targets for physical tampering and other attacks.

There are some BCIs that integrate Radio Frequency (RF) communication modules, which use the ZigBee protocol introduced on the IEEE 802.15.4 standard. This integration is particularly advantageous for portable BCI devices, where low power consumption is critical for long-term monitoring applications. ZigBee is beneficial for BCIs that require a robust and long range wireless communication, enhancing the versatility and range of applications. Nonetheless, interference and limited bandwidth can pose challenges, leaving these protocols prone to disruptions in both data integrity and transmission reliability.

Table 2. Commercial BCIs and their supported communication protocols.

Device Name	Channels ^a	Signal Type	Supported Proto- cols	Applications
OpenBCI Ganglion	4	EEG, EMG, ECG	Bluetooth LE, USB, ZigBee (cus- tom)	Research, neuro- feed- back
NeuroSky MindWave Mobile 2	1	EEG	Bluetooth LE, Blue- tooth 4.0, ZigBee (cus- tom)	Education, gaming, per- sonal
Emotiv Epoc X	14	EEG	Classic Blue- tooth, USB dongle	Research, gaming, neuro- market- ing
Muse 2	7	EEG	Bluetooth LE	Meditation, mindful- ness
g.tec g.USBamp	16–256	EEG, EMG, ECG	USB, ZigBee (cus- tom)	Clinical diag- nostics, research
Neurable (MW75)	6	EEG	Bluetooth LE, USB, ZigBee (cus- tom)	AR/VR control, gaming
NextMind	1	EEG	Bluetooth LE	AR/VR, hands- free control
BrainCo FocusCalm	4	EEG	Bluetooth LE	Education, cogni- tive training
Kernel Flow 2	Multiple	NIRS	Wi-Fi, USB	Cognitive research, clinical
Bitbrain Diadem	8–32	EEG	Wi-Fi, Blue- tooth LE, USB, ZigBee (cus- tom)	Research, clinical use

^a Number of channels (electrodes).

4. BCI Vulnerabilities and Challenges

The predominant types of brain waveforms utilized in the development of EEG-based BCIs include: P300 waveforms, Steady-State Visually Evoked Potentials (SSVEP), Error-

153

154

155

Related Potential (ErrP), Event-Related Desynchronization/Resynchronization (ERD/ERS), and alpha waves [5,7]. Among these, P300 signals appear prominently in commercial EEG applications. The P300 waveform is a positive electrical brainwave detected roughly 300 milliseconds after a user is stimulated. This predictability poses a significant security risk, leaving BCIs open to spoofing and other forms of cyberattacks [10].

Researchers have identified a range of additional cybersecurity threats that jeopardize P300-based and other BCI devices during the complete operational process. This overview spotlights the vulnerabilities found in current literature, particularly for BCIs communicating via Bluetooth Low Energy (BLE), and highlights the critical areas of concern and the potential impact of these threats on the integrity and functionality of BCI systems. Several attacks were identified during the whole BCI process; Bluetooth Connection, Signal Acquisition, Data Transmission, Data Processing, User Application Interaction, and Neural Feedback Loops.

Table 3. Systematic review of BCI cybersecurity attacks reported across the literature. Columns show which sources discuss each attack type.

Cybersecurity Attack	[3]	[7]	[4]	[11]	[2]	[10]
Adversarial attacks	✓				✓	✓
Misleading stimuli attacks	✓					
Cryptographic attacks	✓		✓			✓
Firmware attacks	✓					✓
Battery-drain attacks	✓					
Injection attacks	✓		✓	✓	✓	✓
Malware attacks	✓				✓	✓
Ransomware attacks	✓					
Botnet attacks	✓				✓	
Sniffing attacks	✓				✓	✓
Man-in-the-middle (MitM) attacks	✓	✓		✓	✓	✓
Replay attacks	✓	✓	✓			✓
Social engineering attacks	✓					
Spoofing attacks	✓	✓	✓		✓	✓
Signal tampering		✓	✓	✓		
Eavesdropping		✓				
Data theft			✓			
Denial of service (DoS)			✓			✓
Privilege escalation					✓	
Jamming attacks						✓

Columns correspond to sources: [2–4,7,10,11].

After analyzing and comparing the literature, it is evident that BCIs are susceptible to both traditional cybersecurity attacks, such as Man-in-the-Middle (MitM) attacks—where an attacker intercepts the keys exchanged between devices to eavesdrop on communications—and more specialized neural cyberattacks. We could identify the key vulnerabilities across all the operational phases:

- A) **Bluetooth Connection:** Devices are susceptible to MitM attacks, data sniffing and spoofing due to weak encryption and authentication in BLE protocols.
- B) **Signal Acquisition:** Risk to jamming (interference with legitimate signals), spoofing (introduction of fake signals like P300), and replay attacks (reusing recorded signals to simulate inputs).
- C) **Data Transmission:** Common threats include MitM attacks, cryptographic exploitation and replay attacks.
- D) **Data Processing:** Susceptible to malware, adversarial attacks, injection attacks, and algorithm manipulation.

- E) **User Application Interaction:** Vulnerabilities include exploitation through malicious applications, privilege escalation, spoofing, and social engineering, which can lead to unauthorized system control.
- F) **Neural Cyberattacks:** Susceptible to tampering, injection attacks, overstimulation (neural flooding) and inhibition (neural jamming).

Table 4. Systematic review of BCI cybersecurity challenges highlighted across the literature.

Cybersecurity Challenge	[3]	[7]	[4]	[11]	[2]	[10]
Data confidentiality	✓		✓	✓	✓	✓
Data integrity	✓				✓	✓
Service availability	✓		✓		✓	✓
Physical and psychological safety	✓					
Neural privacy	✓		✓			✓
Technological constraints	✓	✓				
Dynamic security updates	✓					
Secure-by-design development	✓		✓	✓		✓
Protection against malicious stimuli	✓					
User training		✓		✓		
Low signal-to-noise ratio (SNR)		✓				
Scalability		✓			✓	✓
Secure signal transmission			✓	✓		✓
System robustness			✓	✓		
Real-time analysis			✓			
Standardization			✓		✓	✓

Columns correspond to sources: [2–4,7,10,11].

On the other hand, BCI devices face a multidimensional security challenge, due to a lack of standardization and the absence of Security-by-Design principles. Neither manufacturers nor regulatory bodies have adequately addressed these challenges. After analyzing the vulnerabilities, challenges and existing proposals, our contributions are as follows:

- **Passive Attack Evaluation:** We performed a passive attack on BCIs to evaluate and understand the vulnerabilities they pose. We also conducted additional analyses to comprehend the critical features that impact their level of security.
- **Technical Analysis of Commercial BCIs:** We have performed an analysis of the technical aspects of BCIs that are currently on the market, to assess their security levels and compare their performance.
- **Security Scoring Framework:** We designed a security scoring framework based on previous work from authors Silva-Trujillo et al. [12] to propose the minimum requirements that a BCI must meet to be categorized as secure.

We could also identify some of the recent efforts to secure BCIs. Among them, one approach is a blockchain framework that has been proposed to secure communications by leveraging decentralization, immutability and smart contracts to protect data integrity [2]. However, these solutions often impose significant computational resources and introduce latency, making them less suitable for real-time application and for current BCI devices on the market. Similarly, other studies in the literature have implemented OS kernel modules coupled with user space frameworks to harden system level defenses and mitigate vulnerabilities across the software stack [11]. While these approaches offer improved control and monitoring of operations, they also introduce increased complexity and require specialized expertise which may not be feasible for many BCI implementations. Although the integration of machine learning algorithms for threat detection is promising, current

IoT devices and BCIs do not possess robust computational power necessary to run such algorithms efficiently. For these reasons, our work instead focuses on enhancing the pairing process, providing a more practical and immediate enhancement to BCI security.

5. Bluetooth Low-Energy Pairing Methods

In this section, we present the pairing methods for Bluetooth Low Energy (BLE), introduced in the Bluetooth 4.0 specification. Since its adoption, most devices can support both Bluetooth Classic and BLE (dual mode). This is the most used communication protocol within the commercial BCI devices, due to its two key features; low energy consumption and Generic Attribute Profile (GATT)-based data transmission [13]. Consequently, it is crucial to understand the level of security of each of their pairing methods, to assess and implement a Security-by-Design approach when manufacturing these devices.

The Secure Simple Pairing (SSP) mechanism was developed as a part of the Bluetooth Standard. The main goal of SSP is to establish the link key between two Bluetooth Devices. During this process, SSP uses the Elliptic Curve Diffie-Hellman (ECDH) public key algorithm to protect connections from MitM attacks. As a countermeasure, SSP offers four different modes of authenticated key exchange, each varying in security depending on the technical design and Input/Output capabilities (IOCaps) of the devices: Just Works, Numeric Comparison, Out-of-Band (OOB), and Passkey Entry [14].

- A) **Just Works.** This is the least secure pairing method, as it allows the pairing process to be done without user interaction. It is commonly used when at least one of the pairing devices lacks a display or keyboard for entering digits. Unfortunately, many BCIs rely on this method, leaving them unprotected against MitM attacks.
- B) **Numeric Comparison.** This method is used when both devices can display a 6-digit number on their respective screens. The user provides a YES or NO response if the numbers match. This method presents a better level of security compared with Just Works; nevertheless, the designs that BCIs possess nowadays do not offer a screen to display data to be used during the pairing process.
- C) **Passkey Entry.** Designed for the devices with input capabilities, but no screen to display. This method uses a 4-digit or 6-digit numeric passkey, which is generated on one device and must be entered on the other one. A Temporary Key (TK) is generated after the passkey is shared between devices. It is recommended to use a 6-digit passkey to reduce the likelihood of an attack. Some BCI devices use a 4-digit passkey, however sometimes all digits are set to 0, leaving the pairing exposed to eavesdropping and MitM attacks.
- D) **Out-of-Band (OOB).** This association model applies to devices that support an additional separate channel, either wireless (i.e., Near-Field Communication and QR) or wired, for the pairing process. By exchanging the Temporary Key (TK) through an alternate medium, OOB pairing significantly reduces susceptibility to man-in-the-middle (MitM) attacks, since an adversary would need to compromise both channels simultaneously. As a result, BCIs equipped with OOB pairing represent a notable advancement in security, offering a robust second layer of protection.

Additionally, the National Institute of Standards and Technology (NIST) recommends that manufacturers implement an Advanced Encryption Standard (AES), as it secures even more the data that is being transmitted [15]. Encryption requires pairing, which performs a key exchange between the master and slave devices. Two key exchange methods are available under the Secure Connections Only (SCO) mode for BLE devices: Legacy Pairing (BLE 4.0 and 4.1) and Secure Pairing (BLE 4.2+). The main difference is that Legacy Pairing does not include ECDH encryption, which makes it vulnerable to eavesdropping attacks. However, in Bluetooth Classic versions 2.1 and 3.0, Secure Simple Pairing (SSP) is used.

This method is less secure than devices that support SCO, emphasizing the need for current commercial devices to adopt the latest encryption and pairing methods, to mitigate risks effectively [13].

6. Passive Attack Test

In this project, we conducted an experiment as a passive attacker to exploit the vulnerabilities of the Bluetooth protocol during the pairing process of BCI devices. Specifically, we implemented an eavesdropping attack on the exchanged packets. This let us verify the current risks that commercial BCI possess for their users. Capturing and recording transmitted packets, MAC addresses and connection parameters, is a critical step that could facilitate more severe attacks, such as Man-in-the-Middle (MitM).

Two BCI devices were tested during the passive attack:

- I. **NeuroSky MindWave Mobile 2-EEG (MWM2).** The headset has a ThinkGear ASIC chip (TGAT1 ASIC) with a static MAC address. The device poses only a single EEG electrode channel to read neural activity, and relies on Bluetooth Classic and BLE (dual mode) for communication. Although it implements a 4-digit passkey entry during pairing, all digits are set to "0," leaving it vulnerable to cyberattacks.
- II. **OpenBCI Ganglion.** The OpenBCI Ganglion Board is a 4-channel neural interface designed for EEG, EMG (Electromyography), and ECG (Electrocardiography) signal acquisition. It uses the nRF52832 microcontroller and runs on custom OpenBCI firmware. Data is sampled at 200 Hz on each channel and can be transmitted wirelessly to compatible devices via BLE. Additionally, the Ganglion board supports a USB dongle for proprietary communication, enhancing compatibility and security during data transmission.

To execute the sniffing attack, we employed a Nordic Semiconductor Sniffer (nRF52840), to capture the traffic between our BCI devices and a Windows computer. Wireshark was the software that was implemented to capture and analyze the packets that were spotted by our sniffer. All intercepted packets were "LE LL" (Bluetooth Low Energy Link Layer) type, which represents one of the lowest layers of the Bluetooth Low Energy protocol stack. This layer is responsible for medium access, connection establishment, error control, and flow control [16] (i.e., Advertising and Scanning, Connecting, Data Channels, Encryption). Additionally, the Logical Link Control and Adaptation Protocol (L2CAP) provides fragmentation and reassembly for large data packets. SMP layer is responsible for the security aspects, including key management and device authentication. More detailed data from the packets can be identified at the HCI or ATT protocols level.

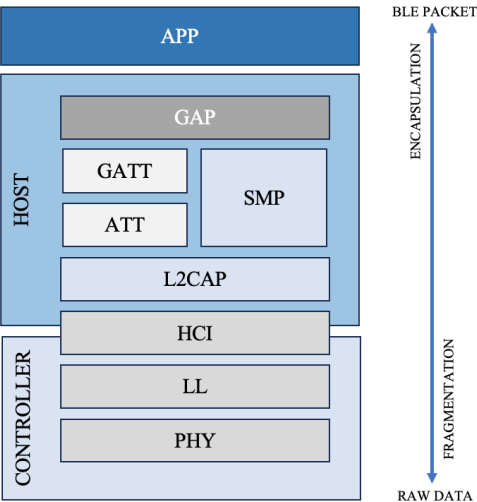


Figure 4. BLE stack.

Among the two tested devices, only the MindWave Mobile 2 was identifiable by our sniffer, as its Unique Identifier was detectable on the packets that were captured. This finding suggests that a more complex attack could potentially be implemented on this particular device, as its packets are easily detectable.

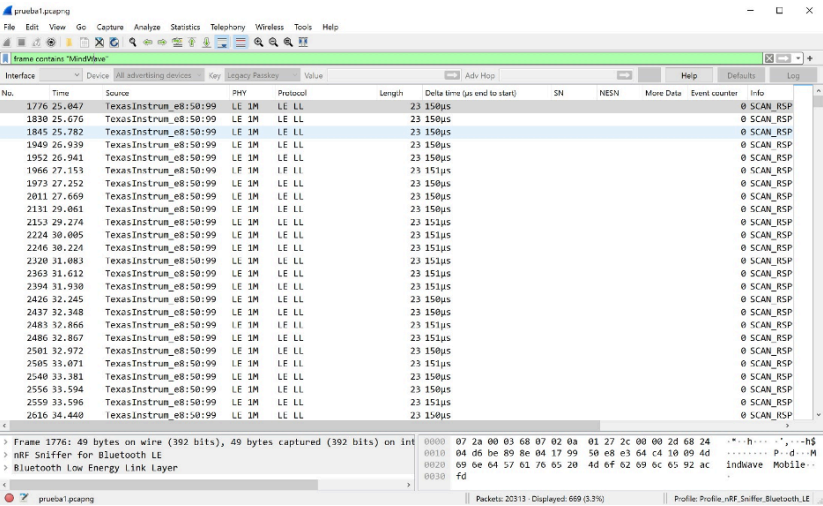


Figure 5. "MindWave Mobile 2" packets captured on Wireshark.

In contrast, the OpenBCI Ganglion device, was not detected by our sniffer. This can be attributed to its USB Dongle, which serves as an additional OOB pairing method. The dongle implements a proprietary protocol to establish communication, leaving it out of reach from our sniffing attack. This result supports our hypothesis that more secure pairing methods, such as OOB, have a direct impact in mitigating these kinds of attacks. Such methods should be considered essential when manufacturers design these devices. Lastly, a co-relation between security and price was observed. The MindWave Mobile 2

costs only one-third of the OpenBCI Ganglion price, suggesting a lack of prioritization by manufacturers to implement a Security-by-Design approach in lower-cost devices, potentially compromising user safety.

7. Scoring Framework

After running the experimental tests, we wanted to deep further and analyze other BCI devices that are currently on the market. We reviewed their technical sheets to obtain critical and relevant data from them. Afterwards, based on a previous framework built for smartwatches by Silva-Trujillo et al. in article [12], we built an specific framework for BCIs that evaluates six features that were especially selected to build our scoring system. The evaluation is grounded in industry standards and the best practices for Bluetooth security. The main goal is to mark the minimum requirements manufacturers require to design secure devices and to help mitigate risks such as eavesdropping, MitM attacks, and device tracking.

Table 5. Commercial BCIs and their Bluetooth features.

Device Name	BL ^a	SC ^b	BLE	JW ^c	PK ^d	OOB	NSA ^e
OpenBCI Ganglion	4.0	LE Legacy Pairing	✓	X	X	✓	X
NeuroSky MindWave Mobile 2	2.1	Secure Simple Pairing	✓	X	4-dig	X	X
Emotiv Epoc X	5.0	LE Secure Connections	✓	X	X	✓	X
Muse 2	4.2	LE Secure Connections	✓	✓	X	X	X
Neurable (MW75)	5.2	LE Secure Connections	✓	✓	X	X	X
BrainCo FocusCalm	5.0	LE Secure Connections	✓	✓	X	X	X
Bitbrain Hero	2.1	Secure Simple Pairing	X	✓	X	X	X

^a Bluetooth Protocol. ^b Secure Connection. ^c Just Works. ^d Passkey Entry. ^e Non-Static Address.

1. **Bluetooth Low Energy.** It is an essential protocol for IoT and wearable devices such as BCIs due to its low power consumption and security improvements over Bluetooth Classic. Devices using BLE are awarded 5 points, as they meet modern standards for secure communication. On the other hand, devices without BLE receive only 1 point, to reflect their limited capacity for a secure, power-efficient application.
2. **Secure Connections.** By using authenticated pairing and Elliptic Curve Diffie Hellman (ECDH) key exchange, the Bluetooth Secure Connections protocol significantly strengthens defenses against threats such as man-in-the-middle (MitM) attacks. BCI devices that use LE Secure Connections earn 3 points, as this is currently the highest standard available. LE Legacy Pairing, while still being a secure method, receives only 2 points, due to its reliance on older encryption methods. The least secure is Simple Pairing, only receiving 1 point, as it lacks robust protection against eavesdropping and MitM attacks.
3. **Just Works Association Model.** As we discussed earlier in the paper, this pairing method is insecure because it does not require authentication during the pairing process. Devices that avoid this association model are rewarded 2 points, while devices that include it are given only 1 point. This scoring encourages manufacturers to prioritize alternative association models, such as Passkey Entry or OOB.
4. **Passkey Requirement.** This association model boosts security by introducing an additional layer of user authentication. A 6-digit passkey, for example, raises the total combinations from 10,000 to 1,000,000—making it considerably safer than its 4-digit

- counterpart. Devices implementing a 6-digit passkey receive 5 points, while those using a 4-digit passkey are rewarded with only 2 points, as the gap between them is considerable. Devices with no passkey functionality only get 1 point.
5. **Out-of-Band (OOB) Pairing.** This is one of the most secure association models, as it requires an alternative communication channel to exchange pairing data. Some BCI devices use an external USB dongle to provide the connection between them, securing the pairing and the transmission of data. Devices that support OOB pairing receive the maximum score of 3 points, as we consider it to be a critical function to implement while designing BCI devices. Those without this feature receive only 1 point.
 6. **Non-Static Address.** Although not commonly used in BCIs, it is already prevalent in other IoT devices, where randomizing addresses makes it more difficult for attackers to trace or identify specific devices over time. BCIs implementing non-static addresses are awarded 2 points, while those using normal static addresses are given only 1 point. Although this feature is not critical for pairing security, it provides additional protection against passive tracking and could help manufacturers to strengthen their security design.

Table 6. Scoring framework criteria for BCI Bluetooth security features.

Criterion	Scoring System	Notes
Bluetooth Low Energy (BLE)	Uses BLE: 5 points No BLE: 1 point	BLE is essential for low power consumption and improved security over Bluetooth Classic.
Secure Connections	LE Secure Connections: 3 points LE Legacy Pairing: 2 points Simple Pairing: 1 point	LE Secure uses authenticated pairing with ECDH, providing stronger defense against MITM attacks.
Just Works Model	Avoided: 2 points Used: 1 point	"Just Works" lacks authentication, so its use lowers security.
Passkey Requirement	6-digit passkey: 5 points 4-digit passkey: 2 points No passkey: 1 point	More digits greatly enhance the security of the pairing process.
Out-of-Band (OOB) Pairing	OOB supported: 3 points Not supported: 1 point	OOB pairing adds an extra secure channel for data exchange, reducing the risk of attacks.
Non-Static Address	Non-static: 2 points Static: 1 point	Randomized addresses help prevent device tracking and enhance overall security.

After reviewing these six features across seven commercial BCI devices, we developed a comparison table (Table 6) to provide an insightful overview and illustrate how closely each device adheres to current Bluetooth security requirements. From these findings, we developed a scoring framework (Figure 7) based on the most critical parameters that we selectively chose, and that helps as a guide for analyzing and assessing BCIs security level. The framework sets a minimum score of 14 points out of 20, representing the minimum requirements a BCI must meet to be considered as a secure device. Features such as BLE pairing and Secure Connections are considered important due to their critical role in mitigating risks and cyberattacks. Although less commonly adopted in current BCI devices, OOB pairing is also considered a key factor for achieving the highest level of

security, as it gives an extra layer of safety during the pairing process. By defining this scoring benchmark, manufacturers can use it as a guide for integrating vital Bluetooth security features into future BCI devices. The framework also serves as a valuable tool for regulators to assess the security level of devices currently available in the market.

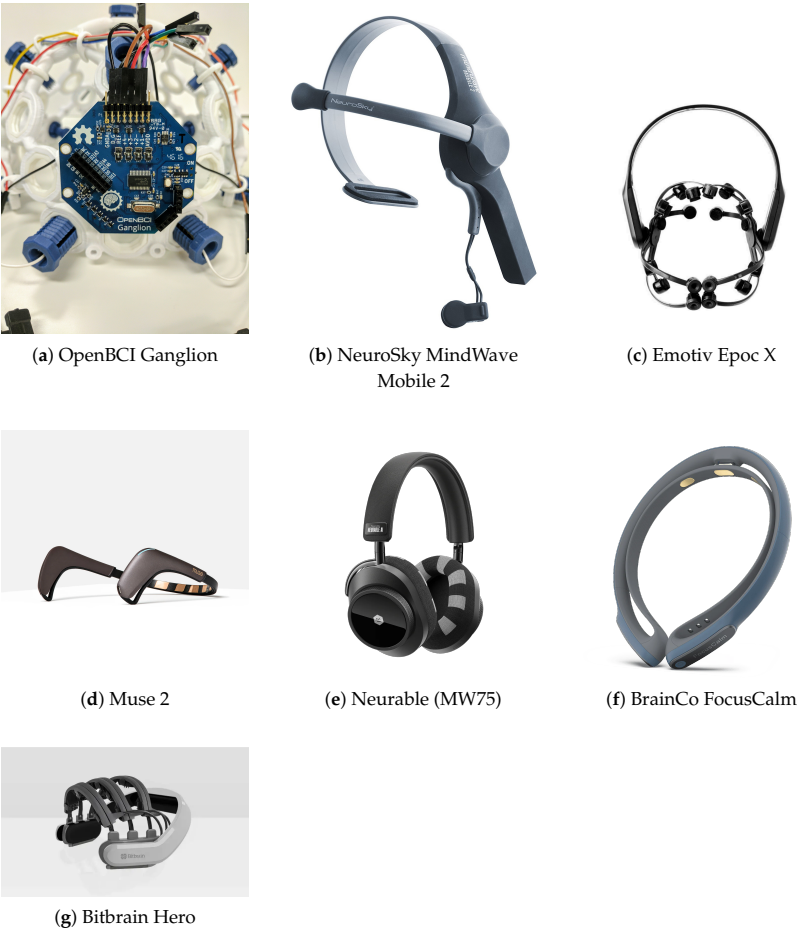


Figure 6. Commercial BCI devices evaluated in this study: (a) OpenBCI Ganglion, (b) NeuroSky MindWave Mobile 2, (c) Emotiv Epoc X, (d) Muse 2, (e) Neurable (MW75), (f) BrainCo FocusCalm, (g) Bitbrain Hero.

Among the seven evaluated BCI devices (Figure 6), only two of them surpassed the proposed minimum requirements. The Emotiv Epoc X emerged as the most secure, achieving the highest score of 15 points, thanks to its robust implementation of LE Secure Connections and OOB pairing. Similarly, the OpenBCI Ganglion, which we used during the passive attack experiment, met the minimum security threshold, making it a reliable option for customers. In contrast, devices like the NeuroSky MindWave 2, Muse 2, and BrainCo FocusCalm fell just below the threshold due to their reliance on less secure pairing mechanisms, and the absence of OOB pairing. The least secure device was the Bitbrain Hero, which lacked essential security features entirely.

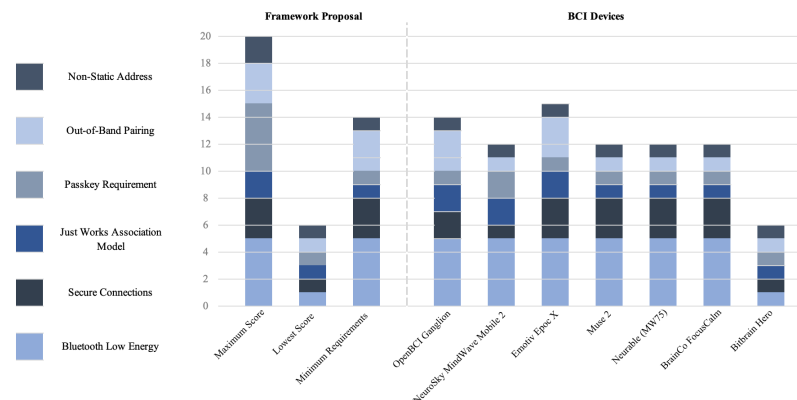


Figure 7. Proposed scoring framework for Bluetooth security in BCI devices.

8. Conclusions and Final Thoughts

The popularity and adoption of BCI devices are increasing in diverse domains, from healthcare and research to daily activities. However, our state-of-the-art analysis and our passive attack experiment, unveiled critical vulnerabilities and challenges in current BCI devices. The lack of standardization and Security-by-Design is largely overlooked by manufacturers and regulators. This issue poses significant risks to the confidentiality of users' neuro data, especially as these devices become more widely accessible. By proposing a scoring framework based on actual Bluetooth security standards, we aim to encourage manufacturers, researchers, and regulators to adopt a Security-by-Design approach when developing these devices, before releasing them on the market. However, we assessed the safety levels of seven commercial BCI devices using our proposed framework, and only two surpassed the minimum security threshold. This outcome highlights the current lack of focus on safeguarding users' neural data during the production of BCI devices. Finally, our ultimate goal is to ensure and safeguard the integrity of users, positioning BCIs as a secure technology for future developments.

References

- Van Erp, J.; Lotte, F.; Tangermann, M. Brain-Computer Interfaces: Beyond Medical Applications. *Computer* **2012**, *45*, 26–34. <https://doi.org/10.1109/MC.2012.107>.
- Khan, A. A.; Laghari, A. A.; Shaikh, A. A.; Dootio, M. A.; Estrela, V. V.; Lopes, R. T. A Blockchain Security Module for Brain-Computer Interface (BCI) with Multimedia Life Cycle Framework (MLCF). *Neuroscience Informatics* **2022**, *2*, 100030. <https://doi.org/10.1016/j.neuri.2021.100030>.
- Bernal, S. L.; Celdrán, A. H.; Pérez, G. M.; Barros, M. T.; Balasubramaniam, S. Security in Brain-Computer Interfaces: State-of-the-Art, Opportunities, and Future Challenges. *ACM Comput. Surv.* **2022**, *54*, 1–35. <https://doi.org/10.1145/3427376>.
- Landau, O.; Puzis, R.; Nissim, N. Mind Your Mind: EEG-Based Brain-Computer Interfaces and Their Security in Cyber Space. *ACM Comput. Surv.* **2021**, *53*, 1–38. <https://doi.org/10.1145/3372043>.
- Korovesis, N.; Kandris, D.; Koulouras, G.; Alexandridis, A. Robot Motion Control via an EEG-Based Brain-Computer Interface by Using Neural Networks and Alpha Brainwaves. *Electronics* **2019**, *8*, 1387. <https://doi.org/10.3390/electronics8121387>.
- Martinovic, I.; Davies, D.; Frank, M.; Perito, D.; Ros, T.; Song, D. On the Feasibility of Side-Channel Attacks with Brain-Computer Interfaces. In *Proceedings of a Security/Privacy Conference*; 2012.
- Abdulkader, S. N.; Atia, A.; Mostafa, M.-S. M. Brain Computer Interfacing: Applications and Challenges. *Egyptian Informatics Journal* **2015**, *16*, 213–230. <https://doi.org/10.1016/j.eij.2015.06.002>.
- Zúñiga-Fajuri, A.; Villavicencio Miranda, L.; Zaror Miralles, D.; Salas Venegas, R. Chapter Seven – Neurorights in Chile: Between Neuroscience and Legal Science. In *Developments in Neurobiology*; 2021; pp. 165–179. <https://doi.org/10.1016/bs.dnb.2021.06.001>.
- Bernal, S. L.; Celdrán, A. H.; Pérez, G. M. Eight Reasons to Prioritize Brain-Computer Interface Cybersecurity. *Commun. ACM* **2023**, *66*, 68–78. <https://doi.org/10.1145/3535509>.

10. Belkacem, A. N. Cybersecurity Framework for P300-Based Brain Computer Interface. In *2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*; IEEE: Toronto, ON, Canada, 2020; pp. 1–6. <https://doi.org/10.1109/SMC42975.2020.9283100>. 415
11. Tarkhani, Z.; Qendro, L.; Brown, M. O.; Hill, O.; Mascolo, C.; Madhavapeddy, A. Enhancing the Security & Privacy of Wearable Brain-Computer Interfaces. *arXiv* **2022**, arXiv:2201.07711. <https://doi.org/10.48550/arXiv.2201.07711>. 416
12. Silva-Trujillo, A. G.; González González, M. J.; Rocha Pérez, L. P.; García Villalba, L. J. Cybersecurity Analysis of Wearable Devices: Smartwatches Passive Attack. *Sensors* **2023**, *23*, 5438. <https://doi.org/10.3390/s23125438>. 417
13. Zhang, Y. Breaking Secure Pairing of Bluetooth Low Energy Using Downgrade Attacks. (Preprint/Technical Report; venue not specified.) 418
14. Haotian, Y. Security Analysis of Bluetooth Secure Simple Pairing Protocols with Extended Threat Model. *Journal of Information Security and Applications* **2023**, *72*, 103385. <https://doi.org/10.1016/j.jisa.2022.103385>. 419
15. Sun, D.-Z.; Mu, Y.; Susilo, W. Man-in-the-Middle Attacks on Secure Simple Pairing in Bluetooth Standard V5.0 and Its Countermeasure. *Pers. Ubiquit. Comput.* **2018**, *22*, 55–67. <https://doi.org/10.1007/s00779-017-1081-6>. 420
16. Siekkinen, M.; Hiiienkari, M.; Nurminen, J. K.; Nieminen, J. How Low Energy Is Bluetooth Low Energy? Comparative Measurements with ZigBee/802.15.4. In *2012 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*; IEEE: Paris, France, 2012; pp. 232–237. <https://doi.org/10.1109/WCNCW.2012.6215496>. 421

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content. 422