

A 3D Virtual Laboratory for Teaching Physical Information Security Devices

Fernanda Ribeiro Martins, Ricardo de la Rocha Ladeira

Instituto Federal Catarinense – Campus Blumenau – Blumenau/SC – Brazil

fernandamartins.rm@gmail.com, ricardo.ladeira@ifc.edu.br

Abstract. *Access to practical Information Security environments and equipment, especially in distance learning and resource-limited institutions, can be challenging. This paper presents a Unity-based 3D virtual laboratory prototype for exploring physical Information Security devices. The current prototype includes two modeled devices on a virtual workbench and basic interactions that allow users to select, rotate, pick up, and release them. A workflow for a Radio-Frequency Identification (RFID) card and tag cloning activity has been designed, while the corresponding reading and writing simulation is under development. The results show that the 3D environment and its basic interactions are functional, but do not yet establish its educational effectiveness, which remains to be assessed.*

Notice: This paper discusses devices that can be misused to violate security and privacy. Their use outside legitimate educational and research contexts is strongly discouraged. This work was developed exclusively for educational purposes.

1. Introduction

Virtual laboratory activities can help students gain a broader and clearer understanding of the subject matter being taught. They can complement the role of physical laboratories and enable activities that would otherwise be impossible due to constraints [Souza *et al.* 2001], such as a lack of physical space or the financial resources needed to acquire equipment [Beraldo *et al.* 2021].

In e-learning, information is often presented in textual form, although some training requires practice. In this case, virtual labs can be an effective solution [Liu *et al.* 2015]. Furthermore, they can complement and enrich in-person laboratory experiences [Souza *et al.* 2001].

Practical experience is essential for consolidating knowledge in the Information Security field. Exclusively theoretical instruction can hinder the understanding of these concepts in practical situations [Willems & Meinel 2012]. Furthermore, educators face the challenge of creating environments that simplify concepts, thereby helping students understand how a real-world environment operates [Thompson & Irvine 2011].

Initiatives that involve carrying out practical security activities tend to focus on digital challenges, such as Hack The Box¹, which addresses privilege escalation and vulnerability exploitation, and on competition platforms, such as TreasureHunt [Ladeira

¹ <https://www.hackthebox.com/>

et al. 2020] and PicoCTF [Chapman *et al.* 2014]. However, comparatively fewer initiatives focus specifically on the interactive exploration of physical Information Security devices. According to [Schreuders *et al.* 2026], security attacks involve both digital and physical systems, and understanding both is essential for training in the area.

Within the context of Information Security, [Lemeshko *et al.* 2020] state that virtual laboratories can be an alternative to carry out practical activities in remote teaching or in situations where there is no access to appropriate equipment, even in person. The same applies to the study of physical security devices, which is often limited to theoretical instruction supported by images and videos. Even in face-to-face classes with access to equipment, difficulties may still arise due to the limited number of devices available.

Considering the limited availability of remote teaching options focused on physical security devices, this work presents a 3D virtual laboratory for teaching about such devices. The environment is designed to support their interactive exploration and the study of their operation and use in security procedures, beyond their presentation as visual objects.

2. Related Work

Many studies have explored the development of virtual laboratories of various types, ranging from interactive two-dimensional simulations to immersive environments based on virtual reality.

[Liu *et al.* 2015] developed a 3D virtual laboratory aimed at teaching physics. The three-dimensional environment includes gauges with dynamic panels, which can be assembled and disassembled. The student can choose to watch an animation of equipment assembly or assemble the equipment on their own, with guidance. The authors highlight that virtual learning systems are typically 2D interfaces, which can reduce immersion and make them less attractive to students. In line with this view, this work proposes a 3D virtual laboratory to support the teaching of Information Security.

[Martins *et al.* 2013] presented the implementation of a low-cost virtual reality laboratory for teaching mathematics in a public school. They used GEO-3D, a pre-existing game, for implementation. Computer lab monitors were selected as viewing devices, while mice and keyboards were chosen for user interaction. This selection aims to use already available resources that, although not immersive, are suitable for most applications. The devices chosen by the authors are in line with the proposal of this work, considering the possibility of making the laboratory available for use on personal computers.

Educational games are also used to teach Security. CyberCIEGE is an educational simulation game whose objective is to teach Security concepts in a simplified and interactive way [Thompson & Irvine 2011]. The game addresses topics related to network security, such as encryption, VPN and SSL, through challenges proposed to players. [Thompson & Irvine 2011] highlight that exploratory interaction

favors practical learning of concepts and reduces the fear of failure during the teaching process.

Cyber Resistance is a prototype of a 2D educational game for teaching Cybersecurity. Players can perform activities such as connecting to virtual machines and containers on computer interfaces and performing offensive and defensive security activities. However, the game does not offer activities with physical security devices [Souza *et al.* 2025]. In contrast, this work focuses on the simulation of physical devices and adopts a three-dimensional approach.

Break Escape is a 2D escape-room-style game that incorporates physical and digital security mechanisms through interactive puzzle challenges, with its preliminary educational effectiveness assessed using the Player Experience Inventory [Schreuders *et al.* 2026]. Unlike Break Escape, which abstracts hardware usage into broader escape-room dynamics, this work focuses on the realistic 3D physical manipulation and functional workflow execution of dedicated security devices.

While prior works address security education primarily through abstract interactions or digital-only mechanics, this proposal integrates direct 3D spatial handling with the step-by-step simulation of device workflows. Spatial handling is relevant because the use of these devices depends on physical gestures and positioning, such as swiping a magnetic card or placing a tag near a reader. By focusing on physical security devices within a dedicated virtual laboratory, this work enables the direct exploration of these tools and their operational principles.

3. Method

To carry out this work, a literature review was conducted, focusing on research regarding virtual and remote laboratories, Information Security education, and related educational games. In parallel, physical devices related to Information Security were identified. The identified devices included magnetic card cloners, RFID card and tag cloners, man-in-the-middle attack devices (WiFi Pineapple and Packet Squirrel), USB command injection devices (USB Rubber Ducky), FM transmitters, signal jammers, lock-picking tools, RFID blockers, and information-gathering and remote access devices (LAN Turtle).

The 3D models for the initial prototype were created using Blender², chosen because it is an open-source tool. Some additional models, such as chairs, computers, and peripherals, were obtained for free via the CGTrader³ platform.

The virtual environment was implemented using the Unity⁴ engine, selected because of its widespread use in games and interactive simulations, including laboratory environments such as the one described by [Resende *et al.* 2024]. The implementation includes lighting configuration, 3D object positioning, and material assignment. The

²<https://www.blender.org/>

³<https://www.cgtrader.com/>

⁴<https://unity.com/>

prototype was built as a standalone desktop application for personal computers, operated with mouse and keyboard.

The initial scene presents the modeled devices on a workbench and allows users to navigate the environment and to select, rotate, pick up, and release the devices. The educational objective is to help undergraduate students understand the purpose, operating principles, and security implications of these devices. Device-specific interactions and explanatory content will be developed to support these learning objectives. Explanatory texts are planned for the interface, with support for multiple languages through a selection menu. Figure 1 summarizes the project workflow.

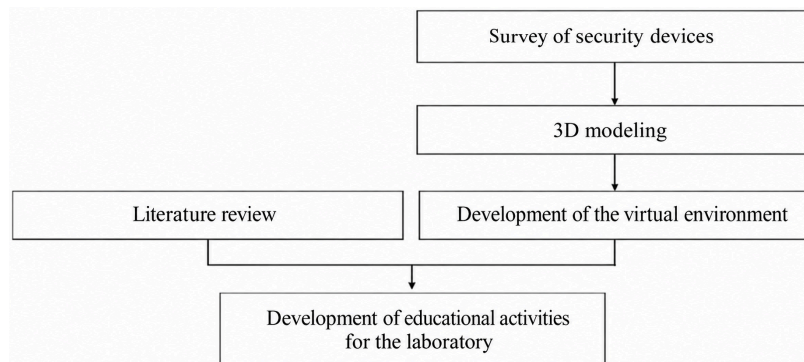


Figure 1. Project workflow.

4. Results and Discussion

Two security devices have been modeled for the project: a magnetic card cloner and an RFID cloner (Figure 2a). Both models were developed based on visual references of real devices obtained from online shopping websites. Complementary elements of the virtual environment, such as tables, walls, doors, and windows, have also been modeled, as shown in Figure 3. The virtual lab allows users to view the devices on a workbench, select them, rotate them using the mouse scroll wheel, and pick them up and release them using the left mouse button (Figure 2b).



Figure 2. Modeled devices and basic interaction: (a) magnetic card cloner (left) and RFID cloner (right), seen from above; (b) RFID cloner held by the user in the virtual environment.

The implemented features provide a functional basis for building an interactive 3D environment for the exploration of physical Information Security devices. A workflow for an RFID cloning activity has been designed, while its simulation of reading and writing operations, the associated explanatory content, and the workflow for the magnetic card cloner remain under development. Therefore, the current results do not establish the educational effectiveness of the laboratory. The Unity project (without the 3D models, textures, and materials, due to file size) and its documentation are available in a public repository⁵, allowing the community to access the implementation and contribute to its development.



Figure 3. Complementary elements of the virtual environment.

5. Conclusion and Future Work

Given the limited number of reviewed works on practices with physical Information Security devices in virtual environments, this work presents a virtual environment aimed at supporting practical Information Security teaching, with two devices currently modeled and incorporated into the prototype. The prototype establishes a technical basis for the planned virtual laboratory, although its educational effectiveness remains to be evaluated. The environment is intended to connect the study of physical security devices with their operation in a controlled virtual setting and may reduce dependence on access to physical equipment.

The next steps involve completing the RFID cloning activity, including the simulation of reading and writing operations and explanatory content, as well as implementing interactions specific to each device, optimizing the 3D models, and adding other security devices. A preliminary educational evaluation is also planned to assess usability, understanding of device operation, and learning outcomes.

Acknowledgements

The authors declare that ChatGPT (GPT-5.5) was used in this work to assist with Unity settings, text revision, and the translation of Figure 1. The authors take full responsibility for the final content of the paper.

⁵ <https://github.com/femrtins/laboratorioSecuranca>

References

- Beraldo, A. L. S., de Oliveira, T., & Stringhini, D. (2021). Laboratórios remotos e virtuais no Brasil com foco no ensino: uma revisão sistemática da literatura. *Renote*, 19(1), pp. 330-340.
- Chapman, P., Burket, J., & Brumley, D. (2014). PicoCTF: A Game-Based Computer Security Competition for High School Students. In 2014 USENIX Summit on Gaming, Games, and Gamification in Security Education (3GSE 14).
- Ladeira, R. R., Obelheiro, R. R., Custódio, R., & Martins, V. (2020). TreasureHunt: um gerador automático de competições de Segurança Computacional. *Revista de Sistemas e Computação (RSC)*, 9(2).
- Lemeshko O., Yeremenko O., Yevdokymenko M., & Kuzminykh, I. (2020). Specifics of creating the Cybersecurity Virtual Laboratory for distance learning. *New Collegium*. 3(101), pp. 41-45.
- Liu, D., Valdiviezo-Díaz, P., Riofrio, G., Sun, Y.-M., & Barba, R. (2015). Integration of Virtual Labs into Science E-learning. *Procedia Computer Science*, 75, pp. 95-102.
- Martins, V. F., Oliveira, A. J. G., & Guimarães, M. P. (2013). Implementação de um laboratório de realidade virtual de baixo custo: estudo de caso de montagem de um laboratório para o ensino de Matemática. *Revista Brasileira de Computação Aplicada*, 5(1), pp. 98-112.
- Resende, H. C., Silva, G. B., & Barbosa, D. M. (2024). UFV Virtual Labs: Plataforma colaborativa e supervisionada de laboratórios virtuais de apoio ao ensino-aprendizagem de ciências da natureza e suas tecnologias. In *Anais do XXXV Simpósio Brasileiro de Informática na Educação (SBIE)*, pp. 651-664.
- Schreuders, Z. C., Alali, L., Idzinski, D., & Shaw, T. (2026). Break Escape: a novel game framework for immersive cyber-physical security education. *Lecture Notes In Networks And Systems*. pp. 34-59.
- Souza, A. L. de, Oliveira, J. C., & Santos, M. P. de L. (2001). Recursos Da Computação Gráfica Para O Desenvolvimento De Um Laboratório Virtual De Teoria Eletromagnética. In *Congresso Brasileiro de Educação em Engenharia*, pp. 171-179.
- Souza, M. V. P., Sangaleti, J. R., Campiolo, R., Almeida, M. S., & Santos, L. A. F. (2025). Cyber Resistance: Protótipo de jogo educacional para ensino de segurança cibernética. In *Workshop de Trabalhos de Iniciação Científica e de Graduação em Andamento – Simpósio Brasileiro de Cibersegurança (SBSeg)*, pp. 305-311.
- Thompson, M., & Irvine, C. (2011). Active learning with the CyberCIEGE Video Game. In *4th Workshop on Cyber Security Experimentation and Test*, 11, pp. 1-8.
- Willems, C., & Meinel, C. (2012) Online assessment for hands-on cyber security training in a virtual lab. *Proceedings Of The 2012 IEEE Global Engineering Education Conference (Educon)*. pp. 1-10. IEEE.