Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security

Mikko Korkiakoski
mikko.korkiakoski@oulu.fi
University of Oulu
Oulu, Finland

Anssi Antila
anssi.antila@hotmail.com
University of Oulu
Oulu, Finland

Jouni Annamaa
jouni.annamaa@gmail.com
University of Oulu
Oulu, Finland

Saeid Sheikhi
saeid.sheikhi@oulu.fi
University of Oulu
Oulu, Finland

Paula Alavesa
paula.alavesa@oulu.fi
University of Oulu
Oulu, Finland

Panos Kostakos
panos.kostakos@oulu.fi
University of Oulu
Oulu, Finland

ABSTRACT

There is a need for creating new educational paths for beginners as well as experienced students for cyber security. Recently, ethical hacking gamification platforms like Capture the Flag (CTF) have grown in popularity, providing newcomers with entertaining and engaging material that encourages the development of offensive and defensive cyber security skills. However, augmented reality (AR) applications for the development of cyber security skills remain mostly an untapped resource. The purpose of this work-in-progress study is to investigate whether CTF games in AR might improve learning in information security and increase security situational awareness (SA). In particular, we investigate how AR gamification influences training and overall experience in the context of ethical hacking tasks. To do this, we developed a Unity-based ethical hacking game in which participants complete CTF-style objectives. The game requires the player to execute basic Linux terminal commands, such as listing files in folders and reading data stored on virtual machines. Each gameplay session lasts up to twenty minutes and consists of three objectives. The game may be altered or made more challenging by modifying the virtual machines. In a pilot, our game was tested with six individuals separated into two groups: an expert group (N=3) and a novice group (N=3). The questionnaire given to the expert group examined their SA during the game, whereas the questionnaire administered to the novice group measured learning and remembering certain things they did in the game. In this paper we discuss our observations from the pilot.

CCS CONCEPTS

• **Human-centered computing** → **User studies**; *Mixed / augmented reality*; • **Security and privacy** → *Usability in security and privacy*.

KEYWORDS

augmented reality, cyber security, educational games

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
AHs '23, March 12–14, 2023, Glasgow, United Kingdom
© 2023 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-9984-5/23/03.
https://doi.org/10.1145/3582700.3583955

ACM Reference Format:
Mikko Korkiakoski, Anssi Antila, Jouni Annamaa, Saeid Sheikhi, Paula Alavesa, and Panos Kostakos. 2023. Hack the Room: Exploring the potential of an augmented reality game for teaching cyber security. In *Augmented Humans Conference (AHs '23), March 12–14, 2023, Glasgow, United Kingdom.* ACM, New York, NY, USA, 5 pages. https://doi.org/10.1145/3582700.3583955

1 INTRODUCTION AND RELATED WORK

Knowledge about cyber threats is crucial at the government and institutional levels. However, there is also an increasing need for improving general public's understanding of this topic to reinforce institutional measures, and to satisfy the interest the public may have on cyber security. Novel methods for increasing public awareness of cyber threats are needed as many traditional methods are failing [6]. Education is the most common context for serious games and gamification. This is due to the benefits these approaches have on learning outcomes, motivation, and engagement. [17, 28, 30].

In this paper, we introduce a design, implementation, and explorative evaluation of an augmented reality (AR) game called Hack the Room. The goal of the game is to teach individuals with little or no expertise in cyber security about the fundamentals of ethical hacking.

Educational games and gamification can provide a more extended, engaging, and motivating environment for learning than the traditional contexts for learning [12, 15]. Digital games can create a fun experience and improve knowledge acquisition. Games allow the creation of more attractive or exciting learning environments, which can be fully or partly digital, as an alternative for or an enhancement of the traditional classroom [5, 8]. AR as a technology fits both purposes. It can be an alternative as it allows remote learning and provides enhancement as it can be used to blend digital, even abstract, data with the physical environment. While AR is still a fairly novel technology for many consumers, it has been noticed to increase user retention and motivation in games and learning applications [1, 3].

Several games and platforms where the purpose is to simulate hacking exist: Hack The Box [7], TryHackMe [34], OverTheWire [10], and SANS Cyber Ranges [21] all offer gamified cyber security training. These and others vary in what aspect of hacking they simulate or aim to teach. Often the purpose is not to teach skills but to raise awareness. HACKING Game [18] is a serious game where the purpose is to aid in security resource allocation. OverTheWire [10]

offers so-called wargames for learning and practicing cyber security. Wargames in the context of cyber security refers to challenges for finding and targeting vulnerabilities. Living Security [32], the Mysteeri, [26], Thales [16], and Infosequre [20] combine cyber security training with escape rooms' game logic. CybAR [2], an AR game, focuses on cyber security threats relevant to its platform: smart phones. These include the usage of public WiFi, weak passwords and susceptibility to social engineering. The game's design is based on technology threat avoidance theory (TTAT) [27]. A survey study with the game showed that people found it useful for learning about cyber security. Chiou et al. [9] developed a mobile AR application to teach children about phishing. The purpose of their application was to teach security related abstract concepts to children early on. Garae et al. [14] took advantage of AR's capability of making invisible visible by creating a mobile AR application to efficiently capture the attention of the user.

While expert tutors might be the best option for advanced learning, digital games are tireless tutors, without restrictions posed by time of the day or location. Therefore they are ideal for early knowledge acquisition and/or for targeting previously unreached learners [25, 31]. This is the potential we aimed at tapping into with our game: Hack the Room.

2 HACK THE ROOM

2.1 Design

A constructionist game design method [22, 23] was used in Hack the Room to promote learning new concepts through grounded and practical approach. The designs were inspired by the games reviewed for the related work (Table 1), such as the ones found from the Hack the Box [7] platform. Our target group were people who are not familiar with cyber security topics. In addition to accessibility and playfulness, the goal was to facilitate knowledge transfer without the presence of a tutor or a teacher, in other words, to create an educational game that takes advantage of the potential of digital learning tools. While using AR was not necessary for our approach, we wanted to leverage the technology's ability to comprehensively visualize data with spatial qualities. The possibility to extend the game into a location-based experience also gave more relevant context for using the Situational Awareness Rating Technique (SART) questionnaire [33], which is not suitable for too restricted task based controlled experiments.

The guiding principles for designing the gameplay and game mechanics were adopted from Kiili's [23] model for educational digital games. The model aims for optimal flow and consequent optimal learning and relies heavily on Csikszentmihalyi's [11] theory on flow. According to Kiili's model the optimal flow is achieved by balancing players' skill levels to immediate feedback and clear goals and challenges. Meaningful challenges in Hack the Room are provided by following the stages of ethical hacking [29]: reconnaissance, scanning, gaining access, maintaining access, and analysis [13].

2.2 Gameplay

The game is played using an AR capable mobile phone. Once the game is started, the instructions are shown to the player (Figure 1).

Table 1: The games that influenced the design of Hack the Room according to their platforms.

Game	Web	VR	AR	Availability*	Mobile	Ref.
Mysteeri 24/7	x	-	-	-	-	[26]
Hack The Box	x	-	-	x	-	[7]
TryHackMe	x	-	-	x	-	[34]
OverTheWire	x	-	-	x	-	[10]
SANS Cyber Ranges	x	-	-	x	-	[21]
TLSCER**	-	-	-	-	x	[32]
CybAR	-	-	x	x	x	[2]
Hack the Room	**-**	**-**	**x**	**x**	**x**	[4]

* If the users need special or custom equipment to play the game
** The Living Security Cyber Escape Room

Figure 1: The initial selection screen once the game is started (left) and instructions on how to scan the surrounding space (right).

After this, the objective of the game is presented to the player in a text overlay. The player then proceeds by moving the phone around and viewing the play area, looking for targets to scan (Figure 2).

Figure 2: View after the game recognizes a scannable area where to add a terminal (left) and the view after a scan is completed (right).

After a target is found and scanned, a computer terminal will appear into the view. Using these terminals (Figure 3), the player needs to complete certain tasks, including listing files, reading files etc. in order to obtain a pass code to the next level.

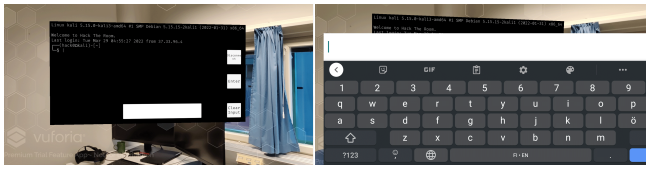

Figure 3: The terminal window (left) and the hovering keyboard the user can use to write commands (right). The users were able to peek around the virtual keyboard to see the console.

After the player retrieves the pass code, they need to make their way to an AR numpad (Figure 4). After entering the correct pass code, the game moves on to the next level. Some questions/tasks are also overlaid into the environment.

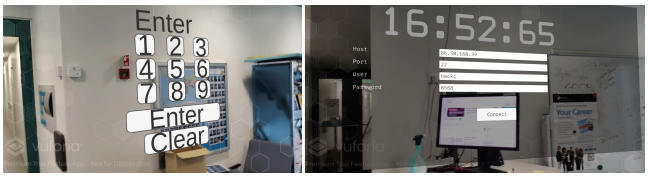

Figure 4: The AR numpad used to enter the obtained pass codes (left) and an introduction to a second terminal in the game after entering the correct pass code (right).

Completing these tasks will again provide the player with a new pass code so they can proceed to the next level. The game ends when the player answers the last question correctly or when the timer (20 minutes) runs out. The time limit was used to avoid player fatigue and limit the whole study procedure to be more manageable.

2.3 Technical Implementation and Architecture

We used the Unity game engine [35] for implementing the game on a mobile phone, OnePlus Nord. The physical environment was scanned using an iPhone 13 Pro and its LiDAR sensor. Vuforia Area Target Creator [19] was then used to create a three-dimensional (3D) play area from the scanned data. Virtual elements such as computer terminals, numpads etc. were then added into this virtual environment using Unity. This allowed tracking for the digital holographic content in AR without added markers, such as QR codes, and introduced elements of exploration and surprise for the players. A secure shell (SSH) connection was used to access virtual machines (VM) via the computer terminals found in the virtual environment. We decided to implement the rapid application development (RAD) method in our development. This decision was made after we noticed how different the gaming experience was between Unity and the actual mobile phone. This approach enabled us to quickly develop a working prototype of the application for the end device. A more detailed description of the technical implementation can be found in [4].

3 PILOT STUDY

This user study was conducted in April of 2022 at the University of Oulu, Finland. The game would start off in an office room and then continue in the hallway for the majority of the gameplay time. The only equipment used in the experiment was a mobile phone (OnePlus Nord), to display the AR content and to interact with the computer terminals, the virtual keyboard and other game contents (Figures 1-4).

There were six participants in this pilot. Three participants were cyber security experts who also had some prior experience with AR applications. The other three were novices with no real experience on cyber security nor AR applications. Five of the six participants were male. The single female participant was part of the expert group. The average ages for the groups were 22 years of age for the novices and 29 for the experts.

The experiment procedure was initiated with the consent form being signed and some basic questions, such as age and gender, and experience about certain applications and knowledge about ethical hacking, answered by the participant. The game would start in an office room after the user was handed the mobile phone. Only the player and the observing researcher would be in the room and the researcher would not communicate with the player unless there was an issue with the phone or if the player asked a specific question about the research procedure. Otherwise, the researcher would only monitor the experiment and take observational notes. Additionally, only if the researcher noticed that the participant had problems figuring out what to do or where to go next, the researcher would give out subtle hints about how to proceed. The office room would serve as a "no distractions" starting point for the experiment and the game would mostly continue on the hallway of the laboratory, although the participants would return to the office room later on for another task.

After completing the game or running out of time, the players would fill in questionnaires. These questionnaires measured gaming experience, SA [33], overall learning experience, and ethical hacking skill and knowledge acquisition [24]. The experts only answered questions about their performance and SA, while the novice group answered all the other questionnaires but not the one regarding SA. We intentionally did not ask the experts the questions about knowledge acquisition and hacking skills because these concepts and methods used in the game are simple and all the experts already know them. So rather, we used the experts as a control group and to evaluate if the game provided a good environment for learning these concepts by administering the SART questionnaire, that can measure the instability, complexity, and variability of the gaming situation. We also recorded completion times for levels and tasks in the game.

4 RESULTS AND DISCUSSION

In this study we wanted to see if our game provides an adequate environment for learning, more specifically if the participants are able to learn about cyber security concepts while playing. In the following, we discuss our findings, however, due to this being a pilot study these findings are inconclusive.

The SART scores suggest that in the expert group, they reported being alert (Table 2, Q4) and concentrated (Table 2, Q5) during the game. For the game situation, they reported only slightly above average complexity (Table 2, Q2). The experts also reported high information quantity (Table 2, Q8) and familiarity of the situation (Table 2, Q9). This suggests they thought the game presented familiar concepts and that they were able to understand the situation well and/or gain information from it. In this group, the participants were aged 28, 30, and one didn't disclose their age. Based on self reporting the group consisted of two males and one female.

Table 2: Expert group SART scores. The SART questionnaire uses a 7-point scale, 1 being very low and 7 very high. Questionnaire items' numbering corresponds to the original [33].

#	1	2	3	4	5	6	7	8	9	SA
1	2	1	3	6	6	2	5	5	7	25
2	5	7	6	7	7	6	6	7	7	22
3	5	4	5	6	6	4	4	4	3	13
avg	4	4	4.67	6.33	6.33	4	5	5.33	5.67	20

For the novice group we were interested in learning outcome. In other words, would the participants remember what kinds of commands they used in the Linux terminals or what did a certain command do. There were five questions that measured if they could remember certain aspects of the game: Q1 *On what port was the SSH service running?*, Q2 *What commands were used in the terminal?*, Q3 *What part of the game was related to the virtual machine?*, Q4 *What was* `nmap` *used for?*, Q5 *What does the* `cd` *command do?*. In addition, there were general questions: Q6 *How would you generalize what you learned during the experiment?*, Q7 *On a scale of 1 to 10, how would you rate the performance of the game?*, Q8 *Did you run into any issues when playing the experiment?*

From Table 3 we can see that two out of the three participants answered all the learning related questions correctly while the third one got 2/5 questions right. So according to these results, it would seem that the participants were learning or at least remembering something from playing the game. The novice group was homogenic consisting of only males aged 21, 22, and 23, which introduces another limitation along with the small sample size.

Table 3: Novice group questions (1 = correct, 0 = false)

#	Q1	Q2	Q3	Q4	Q5
1	1	1	1	1	1
2	1	1	1	1	1
3	1	1	0	0	0
ratio	3/3	3/3	2/3	2/3	2/3

From Figure 5 we can see that for levels 1 and 2 the expert group was faster on average. For the last level it was the novice group that completed it slightly quicker. Although the expert group was quicker in completing the game, the differences were not statistically significant nor were they big. The difference seen in level 2 completion times can be attributed to the novice group members visibly being unsure of what to do next.

5 LIMITATIONS AND FUTURE WORK

This study is clearly a work-in-progress. The sample size was very small and we issued slightly different questionnaires for the groups. The ongoing pandemic still influences the possibility to ethically and safely conduct large scale user studies, so in preparation for the future we will evaluate the study setup.

Our sample size was small, so we cannot present conclusive findings. We also missed an opportunity to interview the participants and gather other more rich qualitative data which would have been more valuable. In addition to recruiting more participants,

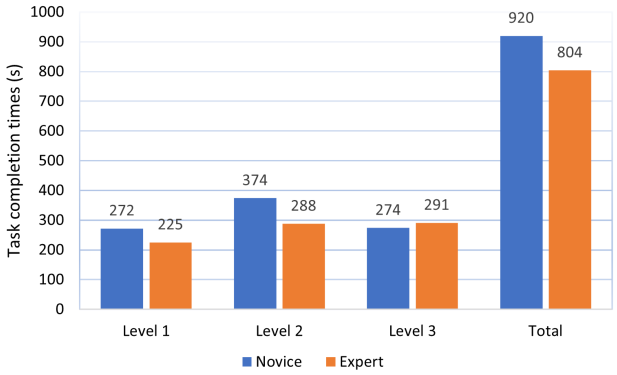

Figure 5: Mean task completion times for both novice and expert groups.

the future work will aim at ironing out the technical issues we encountered, such as the phone losing tracking or scanning of items temporarily not working. These issues could be because the phone we used (OnePlus Nord) is not very powerful and the fact that, in hindsight, the play area could have been scanned more thoroughly. The subpar scan was a result of the play area not containing enough 3D surfaces that the Vuforia engine uses as tracking points. The area also had automated doors that created invisible walls to the scan. To fix this issue, we need to perform a more careful scan of the environment or use a different location. The game could also be ported to an AR headset like the HoloLens 2. This would certainly open up new possibilities in terms of immersiveness and usability via gesture and voice controls. The tasks could also be improved to better scale with the level of knowledge the participants have with different difficulty levels for more experienced users.

6 CONCLUSION

In this paper we describe the motivation, design process and implementation of a mobile augmented reality game called Hack the Room. We conducted a pilot evaluation of the game with six participants who were divided into two groups: those with experience with cyber security and novices. The other metrics used for evaluation produced inconclusive findings; Our main finding comes from the simple observation of how the novices caught up with the experts during gameplay. We consider this an interesting observation considering future work and hope to continue extending the scope of technologies or platforms used for Hack the Room in addition to conducting more research on the topic of using augmented reality games for teaching cyber security.

ACKNOWLEDGMENTS

This research has been supported by Business Finland funded project Reboot Finland IoT Factory 33/31/2018, supported by Academy of Finland 6G Flagship (318927), in addition, the work has been funded by the European Commission grants NESTOR (101021851), IDUNN (101021911) and PRINCE (815362).

REFERENCES

[1] Kati Alha, Elina Koskinen, Janne Paavilainen, and Juho Hamari. 2019. Why do people play location-based augmented reality games: A study on Pokémon GO. *Computers in Human Behavior* 93 (2019), 114–122.

[2] Hamed Alqahtani and Manolya Kavakli-Thorne. 2020. Design and Evaluation of an Augmented Reality Game for Cybersecurity Awareness (CybAR). *Information* 11, 2 (2020), 121. https://doi.org/10.3390/info11020121

[3] Nouf Matar Alzahrani. 2020. Augmented reality: A systematic review of its benefits and challenges in e-learning contexts. *Applied Sciences* 10, 16 (2020), 5660.

[4] Jouni Annamaa and Anssi Antila. 2022. *Hack the room: an augmented reality game for non experts to learn ethical hacking*. Bachelors's thesis. University of Oulu, Faculty of Information Technology and Electrical Engineering, Department of Computer Science and Engineering, Computer Science, Oulu, Finland.

[5] Per Backlund and Maurice Hendrix. 2013. Educational games-are they worth the effort? A literature survey of the effectiveness of serious games. In *2013 5th international conference on games and virtual worlds for serious applications (VS-GAMES)*. IEEE, Poole, UK, 1–8.

[6] Maria Bada, Angela M Sasse, and Jason RC Nurse. 2019. Cyber security awareness campaigns: Why do they fail to change behaviour? *arXiv preprint arXiv:1901.02672* (2019).

[7] Hack The Box. 2022. Hack The Box: A Massive Hacking Playground. {https://www.hackthebox.eu/about-us},journal={HackTheBox}

[8] Elizabeth A. Boyle, Thomas Hainey, Thomas M. Connolly, Grant Gray, Jeffrey Earp, Michela Ott, Theodore Lim, Manuel Ninaus, Claudia Ribeiro, and João Pereira. 2016. An update to the systematic literature review of empirical evidence of the impacts and outcomes of computer games and serious games. *Computers & Education* 94 (2016), 178–192. https://doi.org/10.1016/j.compedu.2015.11.003

[9] Yan-Ming Chiou, Chien-Chung Shen, Chrystalla Mouza, and Teomara Rutherford. 2021. Augmented Reality-Based Cybersecurity Education on Phishing. In *2021 IEEE International Conference on Artificial Intelligence and Virtual Reality (AIVR)*. IEEE, Taichung, Taiwan, 228–231.

[10] OverTheWire community. 2022. OverTheWire: Wargames. https://overthewire.org/wargames/

[11] Mihaly Csikszentmihalyi. 1997. *Finding flow*. Basic Books, New York, US.

[12] Sebastian Deterding. 2012. Gamification: designing for motivation. *interactions* 19, 4 (2012), 14–17. https://doi.org/10.1145/2212877.2212883

[13] EC-Council. 2022. Ethical Hacking. https://www.eccouncil.org/ethical-hacking/

[14] Jeffery Garae, Ryan KL Ko, Janice Kho, Saidah Suwadi, Mark A Will, and Mark Apperley. 2017. Visualizing the new zealand cyber security challenge for attack behaviors. In *2017 IEEE Trustcom/BigDataSE/ICESS*. IEEE, 1123–1130.

[15] Hans W. Giessen. 2015. Serious games effects: an overview. *Procedia-Social and Behavioral Sciences* 174 (2015), 2240–2244.

[16] Thales Group. 2022. Thales Cyber Escape Room. https://www.thalesgroup.com/en/cyber-escape-room Accessed 14.2.2022.

[17] Juho Hamari, Jonna Koivisto, and Harri Sarsa. 2014. Does gamification work?–a literature review of empirical studies on gamification. In *2014 47th Hawaii international conference on system sciences (HICSS)*. IEEE, Waikoloa, HI, USA, 3025–3034.

[18] Arthur H Hendela, Murray Turoff, and Starr Roxanne Hiltz. 2010. Cross impact security analysis using the HACKING Game.. In *ISCRAM 2010*. Information Systems for Crisis Response and Management, ISCRAM, Seattle, WA, US.

[19] PTC Inc. 2022. Vuforia Engine Overview VuforiaLibrary. https://library.vuforia.com/getting-started/vuforia-features

[20] Infosequre. 2022. Infosequre. https://www.infosequre.com/security-awareness-escape-room Accessed 14.2.2022.

[21] SANS Institute. 2022. SANS Cyber Ranges. https://www.sans.org/cyber-ranges/ Accessed 1.3.2022.

[22] Yasmin B. Kafai and Quinn Burke. 2015. Constructionist Gaming: Understanding the Benefits of Making Games for Learning. *Educational Psychologist* 50, 4 (2015), 313–334. https://doi.org/10.1080/00461520.2015.1124022 Cited By :155.

[23] Kristian Kiili. 2005. Digital game-based learning: Towards an experiential gaming model. *The Internet and Higher Education* 8, 1 (Jan 2005), 13–24. https://doi.org/10.1016/j.iheduc.2004.12.001

[24] David R. Krathwohl. 2002. A Revision of Bloom's Taxonomy: An Overview. *Theory Into Practice* 41, 4 (2002), 212–218. http://www.jstor.org/stable/1477405

[25] Wan Shun Eva Lam and Claire Kramsch. 2002. The ecology of an SLA community in a computer-mediated environment. *Ecology of language acquisition* (2002), 141–158. https://doi.org/10.1007/978-94-017-0341-3_8

[26] Laurea, Kajaani University of Applied Sciences, and Häme University of Applied Sciences. 2021. Mysteeri 24/7. https://www.laurea.fi/hankkeet/m/mysteeri-247/

[27] Huigang Liang and Yajiong Xue. 2010. Understanding Security Behaviors in Personal Computer Usage: A Threat Avoidance Perspective*. *Journal of the Association for Information Systems* 11, 7 (07 2010), 394–413. https://www.proquest.com/scholarly-journals/understanding-security-behaviors-personal/docview/734860834/se-2?accountid=13031

[28] Andrzej Marczewski. 2013. Differences between Gamification, Simulations, Serious Games and Games. (2013). https://www.gamified.uk/gamification-framework/differences-between-gamification-and-games/

[29] C. Palmer. 2001. Ethical hacking. (2001), 2. https://doi.org/10.1147/sj.403.0769

[30] R. Abindra Ratan and Ute Ritterfeld. 2009. *Classifying serious games*. Routledge, 32–46.

[31] Jonathon Reinhardt and Steven Thorne. 2016. *Metaphors for digital games and language learning*. 415–430.

[32] Living Security. 2022. Living Security Teams: CyberEscape Online. https://www.livingsecurity.com/cyberescape-online Accessed 14.2.2022.

[33] Richard M Taylor. 2017. Situational awareness rating technique (SART): The development of a tool for aircrew systems design. In *Situational awareness*. Routledge, 111–128.

[34] TryHackMe. 2022. TryHackMe Cyber Security Training. https://tryhackme.com Accessed 14.2.2022.

[35] Unity Technologies. 2022. Unity Real-Time Development Platform 3D, 2D VR & AR Engine. https://unity.com/