Exploring a Board Game to Improve Cloud Security Training in Industry

Tiange Zhao
Siemens AG, Munich, Germany
Universität der Bundeswehr München, Germany

Tiago Espinha Gasiba
Siemens AG, Munich, Germany
Universität der Bundeswehr München, Germany

Ulrike Lechner
Universität der Bundeswehr München, Germany

Maria Pinto-Albuquerque
University Institute of Lisbon (ISCTE-IUL), ISTAR, Portugal

Abstract

Nowadays, companies are increasingly using cloud-based platform for its convenience and flexibility. However, companies still need to protect their assets when deploying their infrastructure in the cloud. Over the last years, the number of cloud-specific vulnerabilities has been increasing. In this work, we introduce a serious game to help participants to understand the inherent risks, understand the different roles, and to encourage proactive defensive thinking. Our game includes an automated evaluator as a novel element. The players are invited to build defense plans and attack plans, which will be checked by the evaluator. We design the game and organize a trial-run in an industrial setting. Our preliminary results bring insight into the design of such a game, and constitute the first step in a research using design science.

2012 ACM Subject Classification Computer systems organization → Cloud computing; Social and professional topics → Computer and information systems training

Keywords and phrases cloud security, cloud control matrix, shared-responsibility model, industry, training, gamification

Digital Object Identifier 10.4230/OASIcs.ICPEC.2021.11

Category Short Paper

Funding This work is partially financed by Portuguese national funds through FCT – Fundação para a Ciência e Tecnologia, I.P., under the projects FCT UIDB/04466/2020 and FCT UIDP/04466/2020. Furthermore, the fourth author thanks the Instituto Universitário de Lisboa and ISTAR, for their support.

1 Introduction

Cloud computing is a relevant and important architecture to provide IT services. The promised value of cloud service providers (CSP) is to provide high levels of service and security and save business costs. Significant players have dedicated themselves to provide cloud-based solutions to the customer. MindSphere [11] is an example of industrial Internet of Things (iIoT) as a service. It powers IoT solutions from the edge to the cloud. A cloud solution can also be found in Siemens' health care industry. Teamplay [15] is cloud-based network aimed to bring together health care professionals in a team effort. The number and volume of applications and systems that are deployed and maintained in the cloud increases.

Cloud-based systems are exposed to security threats as listed in [3] such as nefarious use of cloud services and lack of cloud security architecture and strategy. The current standards [2, 7] and guidelines [4, 1] on cloud security describe the roles and responsibility in cloud

Second International Computer Programming Education Conference (ICPEC 2021).
Editors: Pedro Rangel Henriques, Filipe Portela, Ricardo Queirós, and Alberto Simões; Article No. 11; pp. 11:1–11:8
OpenAccess Series in Informatics
OASICS Schloss Dagstuhl – Leibniz-Zentrum für Informatik, Dagstuhl Publishing, Germany

computing. These standards and guidelines are currently communicated to developers and managers largely by means of security training. It becomes imperative that a company helps its developer and manager understand the importance of cloud security and more precisely how it relates to daily work. Despite the many measures taken, cloud security awareness needs to be improved. We propose a serious game to address this challenge. Our research interest is to design a serious game to facilitate the training of developers and managers about cloud security, especially the roles and responsibilities and the collaboration between cloud service provider and customer. This work presents a preliminary result of a table top game prototype that is designed to introduce fundamental concepts in cloud security.

The research contribution of this work is to propose a possible serious game prototype to increase awareness in cloud security within industry setting and provides the result of game trial-run to verify the proposed prototype.

This article is structured in the following sections: section 2 introduces the related work in area of serious games in information security. Section 3 summarizes the method we use in our research. Section 4 describes the design of our game including the evaluator as a novel element in the prototype. Section 5 shares the feedback we collected from our trial run and our thinking upon it. Section 6 concludes this work and give an outlook into the future research direction.

2 Related Work

This article contributes to the understanding of the design of serious games to increase cloud security. The review of serious games in cyber-security by Shostack [14] demonstrates number and amount of serious games in the domain of cybersecurity.

Shostack presented in [13] a card game *Elevation of Privilege* that draws developers into threat modeling, whose importance used to be underestimated. By designing a cyber-physical systems game, Frey et al. [8] studied the information security field's decision-making process. Romand-Latapie pointed out in [12] that a role-playing game similar to *Dungeons and Dragons* was helpful in training neophyte audience to the basic principles of computer security. They might include cloud computing as a single element in the game design. Still, cloud computing's specific security topics are not addressed, such as shared responsibility model, cloud-specific threats and mitigation.

3 Method

Our research approach is guided by the design science paradigm according to Hevner et al. [9]. The method literature on design science describes the design of a useful artifact as a creative search process for a useful solution.

This paper presents a first step in the creative design process towards a serious game that raises awareness for cloud security among users of industrial cloud services. The design process includes various brainstorming sessions in which the topic “cloud security” and first ideas of a game and design principles of a game (cf. Sect. 4) were developed. The topic was chosen to be able to draw from professional experiences as well as game design and security expertise from the various authors of this paper. It was also chosen because of its relevance in industrial settings.

This first game has been designed in early 2021. A first game run with participants and observers with research interest and knowledge in security topics of cloud service provision was organized in February 2021. We collected the data anonymously and the participants consented to take part in our study. The data collected in participatory observation was analysed, using as source the recorded material of the game session. This paper represents the state of the discussion after data analysis and reflection on next steps in the design process.

4 Game Design

The initial design elements and the game prototype are introduced in this section.

4.1 Initial design elements

In the first brainstorming sessions, the topic "Cloud Security" was identified and the format of the game: it should be a board game that can either be played face-to-face or as a virtual session to accommodate for the restrictions imposed by the COVID crisis. It was also determined that it should take into account the insider perspective of non-compliance with security policies.

By its nature, cloud security provides several elements that could be built into a board game: 1) Cloud security is a constant fight between defender and attacker. 2) For both defender and attacker, there are some constraints on resources. 3) Defenders might have different responsibilities determined by the role they play in cloud security. 4) Attackers could take cloud-specific attack actions to take down cloud assets. Using the elements above together, we can build a board game prototype that is geared to help trainees gain a better understanding on cloud security.

In the design phase, the following core features are identified. The game prototype aims to address those features:

Feature 1: Cloud Security Kill Chain. As Assante et all. mentioned in [5], Cyber attackers do not target systems in single incident and breach. Attackers in cloud security incidents plan the attack step by step. In the game, the attack element should consist of at least several phases instead of a "single shot".

Feature 2: 100 percent security does not exist. Due to constraints on resources, in reality we never aim at 100 percent security in products and solutions. A correct countermeasure does not remove the threat completely. For example, implementing a strong password policy is considered an effective countermeasure to abusing credential. Strong password policy as a countermeasure does not eradicate the threat completely, just lowers the risk. Therefore the defending element should not guarantee any 100 percent security in the game.

Feature 3: Defense-in-depth helps. Use of defense-in-depth strategy, as Kuipers et al. advice [10], in general, improves protection against cyber-threats. Due to the uncertainty of attacker's move, defense-in-depth strategy covers more possible attacks and should be encouraged in the game. The game prototype should address defense-in-depth strategy too.

4.2 Game Process

The game prototype requires a Game Master (GM), who organizes and hosts the game. Before the game starts, the GM explains the rules and the process to participants.

The idea of the game is that defender team develops a defense plan and the attacker team an attack plan. They use a board in which they place cards to model attack and defense plan. Attackers and defenders can only place a limited set of cards. This reflects that in reality neither attacker nor defender have unlimited resources and need to prioritize accordingly.

This development of attack and defense plans is done in teams. Teams use breakout rooms to discuss and develop plans.

There are in total 40 cards, of which 24 cards are made available to defender team and 16 to the attacker team, as table 1 shows. Each card of defender team is printed with one countermeasures to secure cloud assets, for example, "Network Segmentation" or "Information Encryption" (see figure 2). Each card of attacker team has one attack action on cloud assets, for example, "Network Service Discovery" or "Monitoring Escaping" (see figure 3).

Figure 1 presents the phases of the game as a flow chart.

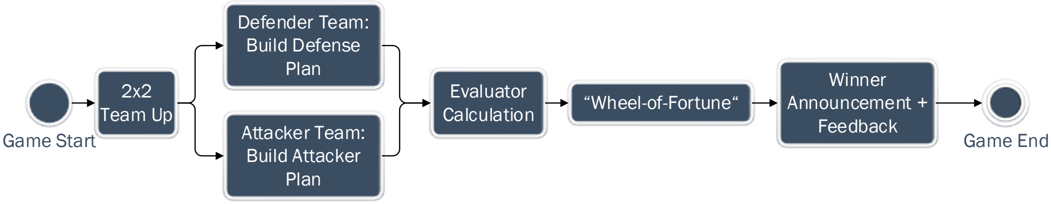
Game Start
2x2 Team Up
Defender Team: Build Defense Plan
Attacker Team: Build Attacker Plan
Evaluator Calculation
"Wheel-of-Fortune"
Winner Announcement + Feedback
Game End

Figure 1 Game Process in Flowchart.

At the beginning of the game, the GM defines the two teams: *Defender* and *Attacker*. In the game, the task of the *Defender* team is to build a defense plan by assigning defense cards to the correct roles: cloud asset owner and cloud asset manager. They should decide to assign which 2 cards to Asset Owner and which 4 cards to Asset Manager. The defender team is not told which ones of the 24 cards belong to Cloud Asset Owner and which ones belong to Cloud Asset Manager. If a card is assigned to the wrong role, it will be excluded from the defense plan and have no effect in the evaluator. Table 1 shows specifically the number of cards of each category. There are two cards that could be assigned to both Asset Owner and Asset Manager. That explains why the sum of the second and fourth row of table 1 is 2 more than the total number of defense cards. Meantime, the task of the *Attacker* is to build an attack plan consisting of three steps: Gain Access, Launch Attack and Make Impact. They will get in total 16 attack cards categorized into the three steps and assign 2, 3 and 1 card(s) to the each step. Both teams have 20 minutes of time to build their defense plan and attack plan.

The attack cards, defense cards and the mapping between them are derived from MITRE ATT&CK [6] and the CSA cloud control matrix [4]. They are typical attack and defense actions in cloud environment.

The finished defense plan will be evaluated against the attack plan by an evaluator. The evaluator implements an algorithm to compute the probability according to which the winner of the game will be determined.

The GM explains the output of the evaluator to participants. For example, which defend card covers which attack card and which attack card is left without any countermeasure. The calculated output from the evaluator is a probability for the Defender Team to survive the attack in the end.

The next step is "Wheel-of-Fortune". That is a virtual spinning wheel with different areas marked as "Attacker wins" or "Defender wins". The area size is determined by the probability calculated in the previous step. In game run-time, "Wheel-of-Fortune" will be spun and the GM announces the winner.

As mentioned above, the evaluator is a novel element in the game process. It will be introduced in detail in the next sub-section.

Table 1 No. of cards for defender team and attacker team.

Defender Team	Total no. of defense cards	24
	No. of defense cards belong to Asset Owner	8
	No. of defense cards to Asset Owner on Defense Plan	2
	No. of defense cards belong to Asset Manager	18
	No. of defense cards to Asset Manager on Defense Plan	4
Attacker Team	Total no. of attack cards	16
	No. of attack cards to chose from for Initial Access	5
	No. of attack cards for Initial Access on Attack Plan	2
	No. of attack cards to chose from for Launch Attack	8
	No. of attack cards for Launch Attack on Attack Plan	3
	No. of attack cards to chose from for Make Impact	3
	No. of attack cards for Make Impact	1

4.3 Evaluator

An evaluator is programmed to evaluate the defense plan against the attack plan through the calculation of the probability of the given defense plan to survive the attack. Throughout different game steps, it shows the reasoning of the final calculation given the defense plan choices against the attack plan. Finally, the evaluator outputs the calculated probability. There are some adjustable parameters for the evaluator such as the number of hints and the single success rate.

Number of Hints

Hint is designed as an assistance for the defender team. It provides the defender team with a correct card assignment to a role in advance of the next game step. By assigning a correct card, it is guaranteed that the card will be included in the defense plan. Based on the observation of the game, the GM can decide whether to give up to two hints to the defender team.

Single Success Rate

The single success rate is the likelihood of a single defense card successfully defend a mapped attack card. It is the same for all defense cards. It reflects the fact that there is no 100% security (Feature 2 in section 4). For example, we normally consider Multi-factor Authentication (MFA) as a valid countermeasure against account manipulation. When single success rate is set to 80%, it means in the game MFA has 80% chance of successfully defending account manipulation attack. In general, the higher the single success rate, the more likely the Defender Team will win. In the trial run, the single success rate is set to 80%.

5 Evaluation of the game

This section presents the result of the first trial run performed in February 2021 in an online format. Three players participated in the game. Two of them are experienced security expert and one of them is university student with basic cyber-security background knowledge. Two university professors were invited as observers. They observed the game without interfering. One of them joined the defender breakout room; the other joined the attacker breakout room.

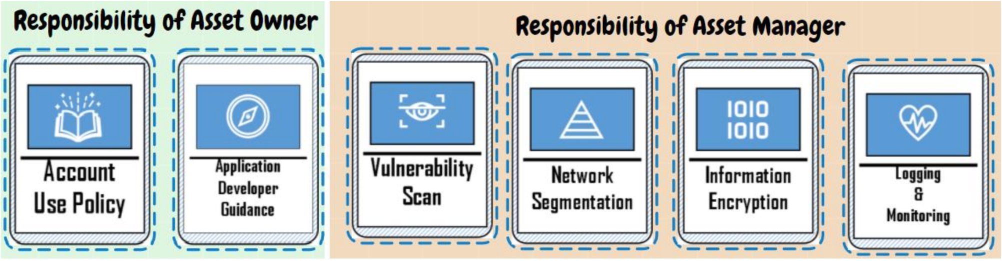

Figure 2 Trial run: a screenshot of of the game board on the defender side.

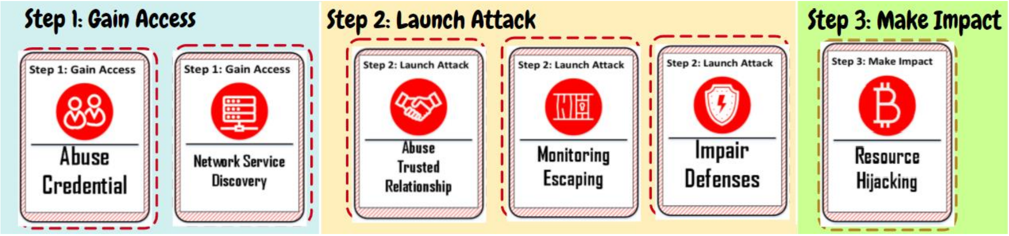

Figure 3 Trial run: a screenshot of of the game board on the attacker side.

5.1 Trial Run Description

Participants were separated in two teams. Each team built their defense or attack plan on an online whiteboard application that was prepared with the cards and game board in advance. Figure 2 and figure 3 are the screenshots of the final defense and attacker plan in our game environment.

The defender team decided to let the asset owner enforce “Account Use Policy” to track information on login attempts and login time and provide “Application Developer Guidance” to minimize security weakness in the development phase. For asset manager, the defender team picked “Vulnerability Scan” to discover potential exploitable software; “Network Segmentation” to isolate critical systems, functions, or resources; “Information Encryption” to protect sensitive information and “Logging & Monitoring” to supervise the overall health and performance of cloud system. All the defense cards were assigned to correct roles, so no card was discarded. To gain access, the attacker team planed to use the card “Abuse Credential” to obtain credentials of existing account and use “Network Service Discovery” to get a list of potentially vulnerable services running on remote hosts. To launch attack, they planned to “Abuse Trusted Relationship” to breach through 3rd party provider; use “Monitoring Escaping” techniques to avoid detection and “Impair Defenses” to maliciously modifies components of a victim environment. In the last step, attacker team chose to make impact by “Resource Hijacking” to leverage the resources of co-opted systems to earn virtual currency.

At the end of the game, both plans were input into the evaluator. The evalutor calculated the final probability of the defense plan against the attack plan to be 96%. The probability was then set to the Wheel-of-Fortune. Despite the attacker team having only a 4% chance of winning, the outcome of the Wheel-of-Fortune was such that this team has won. This was a surprising event for all, but it reflects Feature 2 in section 4 that no defense is 100% secure.

5.2 Results and Discussion

After the trial run, players and observers were invited to exchange their opinions on the game through open discussions. Most of them agreed that the concept was helpful and the game itself was engaging. They also gave feedback on improvement. The following part summarizes the key information of their reviews.

The student participated in the trial run mentioned, *"I think it was pretty cool. It has some cyber-security notions that I still don't really know, so I tried to see both the cheat-sheet and the task. Team environment helped."* We implied from this piece of review that students or beginners can play the game with the prepared cheat-sheet and benefit by teaming up with experienced experts.

One of the security expert suggested, *"The number of rectangles you can assign to the roles represents the resource – you cannot do everything."* When we design the game prototype, we considered that in reality, we could never implement all the countermeasures. They need to be considered individually and prioritized. That reflects the the defensive thinking in real world.

We also got feedback such as *"Why the attack 'Impair Defenses' is covered by the defense 'Loging & Monitoring' is not clear to me..."* As described in section 4, the evaluator checks the mapping between the chosen attack and defense cards. It shows the result in the run-time but does not provide any explanation yet. Further refinement of the evaluator's algorithm and output should be planned for future work.

5.3 Conclusion on the Game Logic and Material

The goal of trial-run is to collect player feedback and draw new ideas for the next design iteration. As we can see from the feedback above, on one hand the participants find the game engaging and reflects pain points in building an effective defense for cloud asset in real world. On the other hand, the constructive feedback was collected and will be addressed in future work. From the designer perspective, the game logic was shown to be reasonable in the trial-run and the prepared material such as cheat-sheet, game board and cards have served their design purposes and helped the players in the game.

6 Conclusion and Future Work

Cloud solutions and deployments are becoming pervasive in the industry. In recent years, the rising number of cloud-related security incidents has shown that companies need to better protect their assets in the cloud. This work proposes a method to address this issue through a serious game, and is a first step in a research being conducted in the industry following the design science methodology. The game is designed based on MITRE ATT&CK [6] and CSA cloud control matrix [4] to reflect real-life situations encountered by companies deploying cloud environments. The goal of the game is to help its players to understand the different dangers that cloud systems face, increase players' understanding of the responsibilities of different roles, and encourage proactive defensive thinking. Towards this goal, a preliminary design of the serious game is presented and is evaluated with real players from the industry in a trial run.

Valuable feedback was collected in the game that enables to steer the design research. To address the constructive feedback collected in trial-run regarding the evaluator, we would like to invite cloud security experts to review the defense and attack on our game card and the mapping between them as one of our next steps. Limitations on the number of players and variations in the participants' background and experience are inherent to this industrial setting and preliminary study. In the future, we would like to invite more participants to join further trial runs and evaluate the level of cloud security awareness before and after playing the game.

References

1 Cloud Security Alliance. Security guidance for critical areas of focus in cloud computing v4.0, 2017. URL: https://cloudsecurityalliance.org/artifacts/security-guidance-v4/.

2 Cloud Security Alliance. Requirements for bodies providing star certification, 2020. URL: https://cloudsecurityalliance.org/artifacts/requirements-for-bodies-providing-star-certification/.

3 Cloud Security Alliance. Top threats to cloud computing: Egregious eleven deep dive, 2020. URL: https://cloudsecurityalliance.org/artifacts/top-threats-egregious-11-deep-dive/.

4 Cloud Security Alliance. Cloud controls matrix v4, 2021. URL: https://cloudsecurityalliance.org/artifacts/cloud-controls-matrix-v4/.

5 Michael J Assante and Robert M Lee. The industrial control system cyber kill chain. *SANS Institute InfoSec Reading Room*, 1, 2015.

6 MITRE ATT&CK. Tabletop security games & cards, 2020. URL: https://attack.mitre.org/versions/v8/matrices/enterprise/cloud/.

7 Carlo Di Giulio, Read Sprabery, Charles Kamhoua, Kevin Kwiat, Roy H Campbell, and Masooda N Bashir. Cloud standards in comparison: Are new security frameworks improving cloud security? In *2017 IEEE 10th International Conference on Cloud Computing (CLOUD)*, pages 50–57. IEEE, 2017.

8 Sylvain Frey, Awais Rashid, Pauline Anthonysamy, Maria Pinto-Albuquerque, and Syed Asad Naqvi. The good, the bad and the ugly: a study of security decisions in a cyber-physical systems game. *IEEE Transactions on Software Engineering*, 45(5):521–536, 2017.

9 Alan Hevner, Salvatore March, and Jinsoo Park. Design science in information systems research. *Management Information Systems Quarterly*, 2004.

10 David Kuipers and Mark Fabro. Control systems cyber security: Defense in depth strategies. Technical report, Idaho National Laboratory (INL), 2006.

11 Dimitri Petrik and Georg Herzwurm. iIoT ecosystem development through boundary resources: a Siemens MindSphere case study. In *Proceedings of the 2nd ACM SIGSOFT International Workshop on Software-Intensive Business: Start-ups, Platforms, and Ecosystems*, pages 1–6, 2019.

12 Tiphaine Romand-Latapie. The NeoSens training method: Computer security awareness for a neophyte audience, 2016. URL: https://airbus-seclab.github.io/dnd/us-16-Romand-Latapie-Dungeons-Dragons-And-Security-wp.pdf.

13 Adam Shostack. Elevation of privilege: Drawing developers into threat modeling. In *2014 {USENIX} Summit on Gaming, Games, and Gamification in Security Education (3GSE 14)*, 2014.

14 Adam Shostack. Tabletop security games & cards, 2021. URL: https://adam.shostack.org/games.html.

15 Dina Simunic, Antun Kerner, and Srecko Gajovic. Digital mediators as key enablers of navigation toward health in knowledge landscapes. *Croatian medical journal*, 2018.