10-20-2023

Teamwork in Cybersecurity: Evaluating the Cooperative Board Game [d0x3d!] as an Experimental Testbed

Crystal Fausett
Embry-Riddle Aeronautical University, fausetc1@my.erau.edu

Joseph Keebler
Embry Riddle Aeronautical University, keeblerj@erau.edu

Teamwork in Cybersecurity: Evaluating the Cooperative Board Game [d0x3d!] as an Experimental Testbed

Crystal M. Fausett & Joseph R. Keebler
Embry-Riddle Aeronautical University

It is crucial to identify the knowledge, skills, and attitudes (KSAs) that contribute to success in cybersecurity teams. We introduce a board game, [d0x3d!], as an experimental testbed designed to create a controlled environment and set of manageable tasks aimed at exploring teamwork competencies that may be relevant to the cybersecurity workforce. [d0x3d!] requires players to work together and share information to retrieve stolen digital assets. The authors aim to improve the efficacy of cybersecurity team training by incorporating modern teamwork theory and measurement. This testbed provides a low-cost and user-friendly platform for training, evaluation, and research.

INTRODUCTION

Organizations are facing a growing concern with the prevalence of cyber-attacks. As per IBM's report for 2022, the average cost of a data breach is a staggering $4.35M, a cost incurred over 9 months – the average time to detect and contain a breach. (IBM, https://www.ibm.com/reports/data-breach). Organizations typically rely on teams to prevent and mitigate cybersecurity threats. The Department of Homeland Security's National Initiative for Cybersecurity Careers and Studies (NICCS) Cybersecurity Workforce Framework (Newhouse et al., 2016) provides a set of work role categories common in the cybersecurity workforce, such as: Security Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate. While there may be variations in the roles and responsibilities of these categories across different organizations and industries, this framework demonstrates the need for teamwork to effectively integrate diverse skillsets to perform cybersecurity actives.

However, teamwork has been a relatively overlooked area in cybersecurity workforce development. This is evident in the knowledge, skills, and aptitudes (KSAs) outlined in the NICCS Workforce Framework. Of 1,060 KSAs identified, less than 10 describe social fit or teamwork competencies (Dawson & Thomson, 2018). It is also exemplified through popular cybersecurity team trainings, which typically take the form of red-team (offense) vs. blue team (defense) exercises. As noted by Simonson et al. (2020), these activities attempt to assess team performance in a binary manner (wins and losses), but largely ignore measurement of teamwork competencies. This has created a challenge for organizations looking to build and train effective cybersecurity teams.

Further, a challenge exists in identifying an appropriate testbed to conduct human-subjects cybersecurity experiments (Mabie & Schuster, 2020). To develop an effective cybersecurity team, it is necessary to identify the teamwork competencies (KSAs) that are relevant to cybersecurity teams. Many sets of team competencies have been proposed (Cannon-Bowers et al., 1995; Cannon-Bowers & Salas, 1997, Salas et al., 2008) but few have been studied in a cybersecurity setting. An effective approach to conducting this research is to observe participants as they complete tasks during simulation-based experiments. However, such a simulation can be prohibitive to many human factors researchers due to development cost, lack of cybersecurity expertise, and access to participants with cybersecurity familiarity.

To address this gap, the cooperative tabletop game [d0x3d!] was repurposed as a cybersecurity testbed for non-experts. While previous research has evaluated the effectiveness of [d0x3d!] as a training and educational tool (Gondree & Peterson, 2013; Gondree et al., 2013; Fendt & Mache, 2014), to our knowledge it has yet to be evaluated as a testbed for studying cybersecurity team competencies. The use of board games as a research tool is not a novel concept. Historically, board games have been utilized to study various aspects of teamwork and collaboration. As an example, Pandemic has been previously used to investigate teamwork constructs such as composition, cognition, communication, cooperation, coordination, coaching, and conflict (Anania et al., 2016). This approach to research has been applied not only to traditional board games but also to video games. Both board and video games provide a controlled environment for observing and analyzing teamwork behaviors, which can provide valuable insights into the development and training of effective teams.

GAMING ENVIRONMENT

Overview

[d0x3d!] is a board game for 1 - 4 players who work together as hackers trying to break into a network. The goal is to collect digital assets and use them to escape the network before getting caught by the network administrators. Every round, the administrators will make the network more secure. If they suspect an intrusion, some machines may be shut down for investigation, the danger level will rise, and the players may get caught. [d0x3d!] is inspired by Forbidden Island, created by Matt Leacock, and therefore has a similar style of gameplay. Figure 1 shows an example of the board game layout.

Description of Game Mechanics

The subordinate goal of [d0x3d!] is to work as a team to infiltrate a network, search for asset shares (pieces of keys), and use those keys to retrieve the assets. After recovering the assets and "escaping," the game ends and the players win.

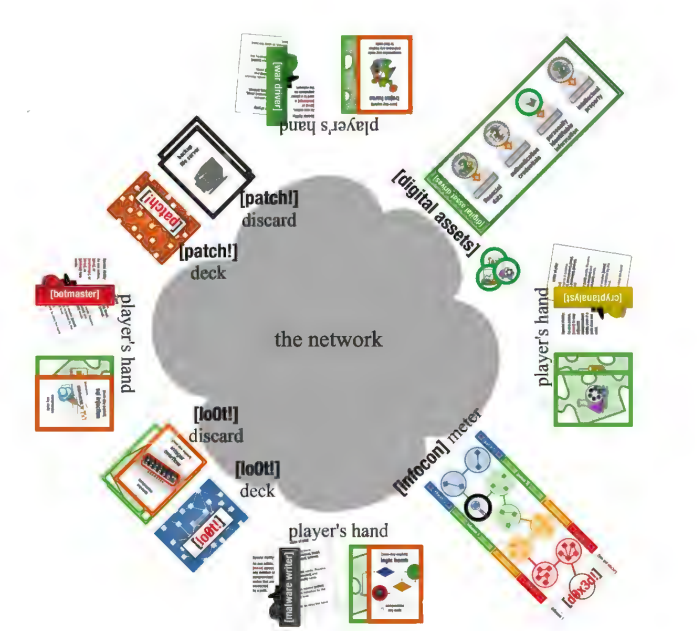

Figure 1. Example game board layout.

The game instructions begin with a story of adversaries stealing digital assets (such as authentication credentials, financial data, intellectual property, and personally identifiable information). Authentication credentials are passwords used for banking or social media. Financial data are information routing numbers or bank account numbers. Intellectual property is items like family recipes. Personally identifiable information is your driver's license and passport number. The adversary locked the digital assets away in a network using a key, split that key into segments, and scattered the segmented keys across servers. The team must then take on the role of various hackers, traversing the network to recover the pieces of keys without getting caught. Once all the key pieces have been assembled, that key will unlock and recover one of the four digital assets. All four digital assets must be recovered before the game can be won. The team members move through the network by compromising network tiles, which compose the game board itself. Figure 2 shows an example of the network tiles that compose the game board.

The adversaries are referred to within the game as "admins," and are constantly monitoring the network. Throughout the game, the admins will patch and/or decommission machines on the network, making it harder to move around. If a player is detected in the network, and cannot escape to another tile, the game ends and the team loses.

Player Roles

[d0x3d!] includes 8 cards representing different hacker roles, each with their own special abilities. The special abilities of the players can alter the rules of the game by allowing game mechanics that the rules would typically prohibit. Like a cybersecurity team, each player has their own set of knowledge, skills, and abilities/attitudes that can be leveraged for success.

Social Engineer. This type of attacker exploits human trust and emotions to gain access to sensitive information, systems, or networks. As a special ability within [d0x3d!], the social engineer can move to *any* compromised node. This is a nod to the ability of a social engineer to bypass the network system entirely, instead exploiting humans to access places they shouldn't. This player role resides on the *internet gateway* tile, which is essential to winning the game.

War Driver. The goal of a war driver is to find open or poorly secured wireless access points to gain unauthorized access to a network and its resources. This ability is exemplified in the game, where the war driver player can give or exchange a card to any player on the network, presumably by exploiting a wireless access point.

Insider. An insider in cybersecurity refers to a person who has authorized access to an organization's information systems, networks, or data because of their job or role within the organization. an insider with malicious intent could use their access to steal sensitive information or disrupt operations. As a special ability, the insider player role can compromise two adjacent nodes on the network with only one action.

Botmaster. A botmaster is a person who controls a network of compromised computers, known as bots or zombies, to carry out various malicious activities. As a special ability, the botmaster can give or exchange two cards as one action. The use of botnets makes it difficult to trace the source of the malicious activities, as the traffic originates from many compromised computers rather than a single source.

Cryptanalyst. Cryptanalysts use mathematical and computational methods to analyze encryption algorithms and to find vulnerabilities that can be exploited to break the encryption. As a special ability, the cryptanalyst can move to any adjacent compromised node, even if a connecting path does not exist.

Malware Writer. A malware writer creates malicious software to harm computer systems or steal sensitive information. As a special ability, the malware writer can move across any number of compromised nodes that are connected by a path.

Figure 2. Example of game board during play. Notice the orange "compromised" network tiles.

Forensic Ninja. Forensic ninjas uncover and analyze the memory of running processes to reveal information. As a spe-

cial action, the forensics ninja can swap a loot card in their hand with one from the discard pile.

Traffic Spoofer. A traffic spoofer manipulates network traffic, typically to disguise malicious behavior such as hiding the origin or destination of the traffic, disguising the content of the communication, or evading security measures.

TEAM COMPETENCIES

There are competencies that are commonly recognized as being predictive of team effectiveness described by Salas et al. (2008). Here, we outline a few of those team competencies, their importance to the cybersecurity workforce, and how those competencies can either be elicited or manipulated through [d0x3d!] as an experimental testbed.

Accurate and Shared Mental Models

Accurate and shared mental models (transactive memory and team situational awareness) refer to team members having a clear understanding of the relationships between the work that the team is doing and how the team members will accomplish that work together (Salas et al., 2005, p. 561). Team members exhibit this competency when they know when others need information they have and anticipate what information their teammates will need. This competency is relevant to cybersecurity teams. Gutzwiller et al. (2016) illustrates this point clearly through the Cyber-Cognitive Situation Awareness model which consists of three layers: the network, the team, and the world. The team level specifically pertains to the awareness of one's role on the team and superordinate goals (Mabie & Schuster, 2020). A cybersecurity incident response team's ability to manage and share information can have a great impact on team effectiveness (Steinke et al., 2015).

Within [d0x3d!], the team competency of accurate and shared mental models may be represented through the special ability that is unique to each player role. For example, the *social engineer* player role has the special ability to move to *any* compromised node, regardless of if a path exists. Each player's special ability can be viewed as a form of specialized knowledge or job role, unique to that player, just as cybersecurity teams are comprised of individuals who have their own specialized knowledge. We posit that teams will be more effective when this knowledge of *who does what* is shared.

In an experimental setting, the competency of accurate and shared mental models could be manipulated by varying the transparency of player roles' special abilities. For example, one condition could involve the introduction of player roles by an experimenter to the group, where all participants are made aware of (and even questioned on) each other's special abilities. In another condition, players would be made aware of their own special abilities but required to learn their teammates abilities organically.

Problem Solving

Problem solving is a competency defined as the ability to understand the difference between the current state of the world versus how it *should* be and figuring out a way to rectify that difference (Salas et al., 2008). Team members exhibit problem solving competencies when they quickly learn new information as needed, plan for things that might go wrong, choose which problems are most important and fix them in the appropriate order, and demonstrate flexibility in their approach. Steinke et al (2015) states that a large part of the work that cybersecurity incident response teams undertake is solving problems in conditions of uncertainty, where a solution is not obvious.

[d0x3d!] inherently is a game of problem solving. Whether team members are figuring out the best way to navigate the network tiles, a strategy for obtaining the stolen assets, or navigating patch effects – team members must work together to solve problems every step of the way.

In an experimental setting, problem solving competencies could be manipulated through the difficulty of the game itself. This could be made easier or harder by varying the infocon level (increasing or decreasing the patch effects), by stacking the deck so that it is either easier (frequent zero-day cards, infrequent intrusion detected cards) or harder (few zero-day cards, frequent intrusion detected cards).

Closed-Loop Communication/Information Exchange

Closed-loop communication is a pattern of communication with three distinct phases:

1. The sender initiates a message.
2. The receiver receives, interprets, and acknowledges the message.
3. The sender follows up to ensure the message was received and interpreted correctly.

This could enhance team performance and would be demonstrated by team members ensuring that messages are received and understood, acknowledging messages they are sent, and cross-checking information.

This communication pattern could be manipulated via [d0x3d!] through prior training of the team on how to use closed-loop communication. Communication and information exchange could also be investigated through [d0x3d!] by varying the virtuality (some team members may be co-located with each other, while others are not co-located and only able to communicate through a virtual platform). This could also be used to investigate human robot teaming, if players believe that one of the players is an autonomous agent through a Wizard of Oz style experiment.

Additionally, within the game, players are required to retrieve stolen digital assets. To do this, one player must discard five loot cards of the same digital asset type on the appropriate network tile. Often, to acquire all five of the same digital asset cards, players must work together to trade and exchange their cards. This means an assessment of what player has what cards, and how many, needs to be made. Communication could be manipulated by requiring players to play with their digital asset cards hidden from other platers (face down) so that players must verbally relay what they have in their hand.

TEAM PERFORMANCE ASSESSMENT

Various measures of team performance are present within [d0x3d!], including win/loss, number of times a tile is compromised, infocon threat level, and assets captured. Below, each of these potential assessments of team performance is discussed:

Win/Loss. Whether the team successfully wins or loses the game is an indicator of team performance. Although this approach may be suitable for fields like cybersecurity that rely on binary outcomes (such as success or failure), this method alone does not provide a meaningful assessment of team performance (Simonson et al., 2020).

Number of times a tile is compromised. This measure captures how well team members can navigate the board and gain access to network tiles by compromising them (flipping them to the orange side). Obtaining and keeping tiles compromised opens new pathways of travel. During gameplay, admins will patch the compromised tiles, reverting them back to their original white side. Therefore, the number of times a tile is compromised is a good measure of team performance assessment.

Infocon Threat Level. The infocon threat level is determined by an "admin token" which increases whenever a machine is patched where a hacker currently resides within the game. The infocon level determines how many patch cards a player must draw per turn, thus a higher infocon level suggests that players have been spotted frequently. This also means a higher difficulty level for players. A higher infocon threat level represents how far the players have progressed through the game, but a win combined with a low infocon threat level may imply that players had a superior strategy that avoided raising threat levels.

Assets Captured. Winning the game requires that all four digital asset tokens have been retrieved, all players occupying the same *internet gateway* tile, and any player playing a zero-day exploit card. This means that players could have retrieved all four digital assets but failed to meet the other two criteria to win the game. Number of digital assets captured is therefore a good measure of team performance, that is slightly more granular than binary win/loss.

EXAMPLE STUDY

Research is currently underway to identify some of the knowledge, skills, and abilities/attitudes (KSAs) that predict success in cybersecurity team roles (Newhouse et al., 2017). Popular methods of cybersecurity team training (such as red team vs. blue team exercises) could be enhanced with the incorporation of modern teamwork theory and measurement (Simonson et al., 2020). To address this need, we are using [d0x3d!] to better understand the team competencies that may be used to improve the efficacy of cybersecurity teams and team training. The [d0x3d!] board game forces players to work together and share information and exemplifies many of the KSAs that appear to be relevant to cybersecurity teams.

This research will use a demographic and background gathering survey to collect relevant data regarding participants video game experience and board game playing habits, as well as general cybersecurity knowledge. This research will also look at team competencies such as joint problem-solving orientation, psychological safety, interdependence, and internal learning behavior, followed by team-based performance metrics to predict and assess each team's success in their activities.

Data will be collected through an observational study using the [d0x3d!] board game as a simulated test bed for team performance. During the data collection session participants will be assigned a role to play in the board game, which will be decided upon at the beginning of each team's participation by the researchers via randomization or set assignment. At the beginning of each data collection session, participants will be asked to complete the demographic survey and cybersecurity knowledge assessment. This is followed by a training session, and then 60-minutes of gameplay. After the game session has been completed, participants will be given a post-survey that requires them to reflect on their experience playing the game. This survey will include items related to team constructs such as joint problem-solving orientation, psychological safety, interdependence, and internal learning behaviors.

After the end of the 60-minute mission, overall performance metrics including win/loss, number of tiles a tile is compromised, infocon threat level, and number of asserts captured will be collected. The researchers will use this data to measure overall success of the mission as well as the efficiency of the team. The data collected about participant demographics, joint problem-solving orientation, psychological safety, interdependence, and internal learning behaviors and these effects on performance will contribute to the field's overall understanding of what factors contribute to success in cybersecurity teams.

CONCLUSION

The cooperative board game [d0x3d!] serves as a valuable experimental testbed for exploring teamwork within the context of cybersecurity. Its low-cost, approachable, and feasible nature makes it a beneficial tool for both researchers and participants, lowering the barrier to entry for studies in this field. The game provides a solution for some of the difficulties encountered in studying cybersecurity, particularly for human factors labs. In this paper, we have discussed a variety of team constructs that can be studied and assessed through [d0x3d!], but it is important to note that this is just a small portion of the potential research that could benefit from this testbed. This highlights the promising potential of [d0x3d!] as a valuable tool for advancing our understanding of teamwork in cybersecurity.

REFERENCES

Anania, E. C., Keebler, J. R., Anglin, K. M., & Kring, J. P. (2016, September). Using the cooperative board game pandemic to study teamwork. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 60, No. 1, pp. 1770-1774). Sage CA: Los Angeles, CA: SAGE Publications.

Cannon-Bowers, J. A., Tannenbaum, S. I., Salas, E., & Volpe, C. E. (1995). Defining competencies and establishing team training requirements. *Team effectiveness and decision making in organizations*, *333*, 380.

Cannon-Bowers, J. A., & Salas, E. (1997). A framework for developing team performance measures in training. In *Team performance assessment and measurement* (pp. 57-74). Psychology Press.

Cost of a data breach 2022. IBM. (n.d.). Retrieved February 27, 2023, from https://www.ibm.com/reports/data-breach

Dawson, J., & Thomson, R. (2018). The future cybersecurity workforce: going beyond technical skills for successful cyber performance. *Frontiers in psychology*, *9*, 744.

Fendt, T., & Mache, J. (2014). Teaching Cybersecurity to Wide Audiences with Table-Top Games. In *Proceedings of the International Conference on Security and Management (SAM)* (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

Gondree, M., & Peterson, Z. N. (2013). Valuing security by getting [d0x3d!]: Experiences with a network security board game. In *6th Workshop on Cyber Security Experimentation and Test ({CSET} 13)*.

Gondree, M., Peterson, Z. N., & Denning, T. (2013). Security through play. *IEEE Security & Privacy*, *11*(3), 64-67.

Gutzwiller, R. S., Hunt, S. M., & Lange, D. S. (2016, March). A task analysis toward characterizing cyber-cognitive situation awareness (CCSA) in cyber defense analysts. In *2016 IEEE International Multi-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)* (pp. 14-20). IEEE.

Mabie, D., & Schuster, D. (2020, December). Lessons Learned in Leveraging Existing Simulations for Cybersecurity Training, Evaluation, and Research. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 64, No. 1, pp. 425-429). Sage CA: Los Angeles, CA: SAGE Publications.

Newhouse, B., Keith, S. S., and Witte, G. (2016). NICE Cybersecurity Workforce Framework. Gaithersburg, MD: National Institute of Standards and Technology

Salas, E., Sims, D. E., & Burke, C. S. (2005). Is there a "big five" in teamwork?. *Small group research*, *36*(5), 555-599.

Salas, E., Rosen, M. A., Burke, C. S., & Goodwin, G. F. (2008). *The wisdom of collectives in organizations: An update of the teamwork competencies.* In E. Salas, G. F. Goodwin, & C. S. Burke (Eds.), *Team effectiveness in complex organizations* (pp. 73-114). Routledge.

Simonson, R. J., Keebler, J. R., Lessmiller, M., Richards, T., & Lee, J. C. (2020, December). Cybersecurity teamwork: A review of current practices and suggested improvements. In *Proceedings of the Human Factors and Ergonomics Society Annual Meeting* (Vol. 64, No. 1, pp. 451-455). Sage CA: Los Angeles, CA: SAGE Publications.

Steinke, J., Bolunmez, B., Fletcher, L., Wang, V., Tomassetti, A. J., Repchick, K. M., ... & Tetrick, L. E. (2015). Improving cybersecurity incident response team effectiveness using teams-based research. *IEEE Security & Privacy*, *13*(4), 20-29.