Influence of Team Communication and Coordination on the Performance of Teams at the iCTF Competition

Shree Jariwala, Michael Champion, Prashanth Rajivan, and Nancy J. Cooke
Arizona State University

Effective team process is critical for the performance of cyber security teams. To examine this, we observed two comparably skilled cyber security teams participating in the International Capture the Flag (iCTF) competition held in December 2011. At the conclusion of the competition, we followed up with a focus group discussion with six members from the two teams. In this paper, we present our findings from the focus group interviews, on the relationship between team level factors and team performance. Findings from the focus group discussion indicate that team level factors such as team communication, coordination, team structure, and leadership play important roles in team performance.

INTRODUCTION

Computers and networks are becoming critical to maintaining our day-to-day lives. Societies rely on computers for tasks ranging from simple banking tasks to large international military operations. Computers store information and perform vital functions, which require protection from malicious attacks for sustained operations. However, the continuous growth of these systems and their tasks are making it increasingly challenging for humans to manage. There are many security vulnerabilities that criminals can exploit, especially in larger systems such as our national infrastructure (for a recent example see Alperovitch, 2011). Whereas the government employs analysts to monitor "alerts" generated from abnormal behaviors in the systems, this task is high in cognitive demand and often surpasses the limits on the amount of data each person can analyze (Champion, Rajivan, Cooke & Jariwala, 2012, D'Amico et al, 2005).

One way to lessen this demand is effective teamwork. A team of people working together can share the cognitive load as long as the load of coordination does not excessively add to their mental load (De Dreu & Weingart, 2003). In the case of cyber security, often there are times in which tasks must continually be interrupted by developing events. Tremblay, Vachin, Lafond and Kramer (2012) showed that people working on a task together do better at dealing with interruptions than a person alone. The question is how teamwork translates into the realm of cyber defense and offense. And if this work is given to a team, will they be more effective than if they worked at an individual level?

There is literature supporting the value of teamwork for cyber offense (e.g. Kraemer, Carayon, & Duggan, 2004; McCloskey & Stanard, 1999). Much of the work has been in context of red (offensive) teams looking for vulnerabilites within corporate systems. However, there is not much information about qualitative processes and coordination of team efforts during these events. The measures of team effectiveness are typically the time it takes to find flags (targets), subjective feelings of the hacking teams, and whether the corporate client understood the results of the event (Kraemer et al., 2004).

Team training on teamwork skills has been shown to be effective for increasing team performance (Salas, Cooke, & Rosen, 2008). It seems often that cyber security teams are simply organized as a team (Champion, Rajivan, Jariwala, & Cooke 2012), but merely bringing individuals together does nothing to improve team performance (Allen & Hecht, 2004). Instead, to be effective, team performance requires communication through which teams process information. This cognitive processing or "team cognition" is directly observable as interactions, including communication itself, between team members (Cooke, Gorman & Winner, 2007).

Coordination is a large aspect of team interaction that can be directly observed and compared between teams (Entin & Serfaty, 1999). The popular Malone and Crowston (1994) definition of coordination is the management of dependencies between activities. In teams, it can be said that coordination is managing the interdependent relations, behaviors and activities of the team. Team structure and communication play major roles in determining how coordination will work within teams.

Team structure is tied to team knowledge of who knows what and who needs what information you have. Champion, et al. (2012) illustrated that teams in cyber security often have loose structures and as a result, lacked enough information to help team members locate needed information. This lack of information is illustrative of poor transactive memory. Transactive memory systems—dividing teamwork by relying on an implicit system of who will learn, remember and needs to know what—are a dynamic component of this structure (Wegner, 1986; Lewis, 2003). Learning where information is "stored" within the team helps people not only consult the right person(s), but also where they should "put" information so that it is appropriately "stored" within the team.

Team structure and communication also play into cooperation which can be defined as how willing team members are to coordinate with each other (Fiore, Salas, Cuevas, & Bowers, 2003). Cooperation depends on factors such as trust and group norms for helping and asking for help. Teams that give feedback are typically more able to cooperate and coordinate.

Capture-the-Flag Competition

In recent years, the value of the capture the flag type events for training and education in the cyber security realm has become increasingly evident (e.g. Doupé et al, 2011; Irvine, 2011). One such competition is the International

Capture the Flag (iCTF) competition hosted by the University of California at Santa Barbara (for more information see Childers et al, 2010). During the 2011 version of the competition, teams had to solve challenges to gain virtual money, create opportunities for infiltration using the vulnerabilities in opponents' systems, capture virtual "flags" from opponent systems, and defend their own network from opponent attacks (please see http://ictf.cs.ucsb.edu/ for more information). This competition provides an opportunity to observe a complex cyber environment in which teams are competing live against each other across the world. This event is described as "a distributed, wide-area security exercise, whose goal is to test the security skills of the participants" (UCSB iCTF, n.d.).

We attended the 2011 iCTF to observe the two teams at Santa Barbara in action. Both teams were comprised of students from a computer security course at the University of Santa Barbara and had comparable skill level and experience. However, Team A outperformed Team B at the competition. Team A reached the 10th position out of 85 teams and finished in the 12th position. Team B did not score in the top 20 groups. Our observations, along with a focus group interview, suggested very different team processes for the two teams. We hypothesize that Team A's better performance is strongly related to better team cognition, the resulting team knowledge system from team processes such as communication and coordination. Support comes from examination of communication and coordination related to team structure, team goals and team motivation.

METHODS

Participants

Two teams, both comprised of 10 students, were observed at the University of California, Santa Barbara who participated in the iCTF competition. All students were enrolled in a graduate level computer security course at the university. All students had a computer science or a computer engineering background. Of the 20 students, 18 were male students and 2 were female students (1 on each team). The 20 students were split equally into two teams: Team A and Team B. Before the start of the competition, we requested the 20 students to voluntarily participate in the study. We informed them that the participation in this study was voluntary. We asked for their consent on being videotaped and observed during the competition using consent forms. All but one student consented to be videotaped.

Four members from Team A and two members from Team B voluntarily participated in the focus group interview following the competition.

Materials

The participation of the two teams in the iCTF competition was captured and stored electronically through a digital video recorder. The focus group session was also captured and stored using a digital video recorder.

At the conclusion of the competition, participants were given a short demographics questionnaire. Fifteen of the 20 participants completed this questionnaire.

Procedures

The scope of these observations did not interfere with the protocols already established by the iCTF competition. The procedures for the competition were that team members were co-located and competed via a virtual private network (VPN). The two locally observed teams were located in a communal computer lab at the University.

At the commencement of the competition, teams performed a variety of tasks to satisfy the requirements of the competition such as gaining administrative access to software and services (i.e. the background system processes) the teams must maintain. The overall competition was eight hours in length.

At the conclusion of the competition a focus group was held in a separate lab within the computer science department. The focus group lasted two hours and consisted of six individuals, with four from Team A and two from Team B. Team leaders from both teams were present for the focus group. Findings from this analysis are presented in the next section.

RESULTS

Game Strategy

There was no difference between the teams in the strategies used to find vulnerabilities in the software system. Both teams examined the source code of the services to identify potential vulnerabilities. Both teams also captured and examined the network traffic from other globally competing teams who exploited their services to identify the vulnerabilities and the process to exploit the vulnerabilities. They then utilized this information to exploit other teams after securing their own system.

Team Structure

Leadership and role assignment during the competition differed between the two teams. The teams themselves were created by the course instructor. In addition to the students from the security course, members from the UCSB Computer Securities Group, who had experience with hacking, were consciously assigned between the two teams, the rest of the students from the computer security course were evenly distributed between both the teams.

Before the competition began, both teams attempted to document individual expertise with systems. The goal behind this was to have a successful and calculated distribution of tasks during the competition. However, neither team completed these documents. Although during the competition, Team A was able to set member roles on the services to exploit and challenges to solve based on then communicated areas of expertise. In part, due to this communication, they were able to dynamically change the structure of the team, as well as the assigned duties of each team member throughout the competition. In contrast, Team B was unable to build effective team roles during the competition.

A notable difference between the two teams was the distribution of leadership. Three members of Team A took leadership roles in addition to their individually assigned roles. Throughout the competition, this dynamic changed based on workload of the individual at the time when a leader was needed. If two or three of the leaders were available for a decision task, they discussed provided information as a committee to come to a conclusion. This method provided very few dissenting opinions, though they did occur when majority rule superseded. An added benefit to this method was that leaders, who had more experience with the capture-the-flag task, were able to concentrate on a task for longer periods of time. Conversely, only one member of Team B took the leadership role. Other members were not willing to participate in the leadership. Although the number of experienced individuals was the same as with Team A, these experienced members were more inclined to simply complete their tasks and not become involved in team leadership. At the same time, the single team leader of Team B, who had prior valuable experience with capture-the-flag tasks, was unable to concentrate on a task for a long period due to frequent interruptions.

Team involvement was another point of differentiation between the two teams. Team A's members were highly involved in the task and maintained information on the current tasks of the team at a high level of abstraction. Often, the team would restructure themselves in order to better facilitate the task at hand. Half way through the competition, these restructurings – becoming more frequent to achieve short-term goals – obtained a level of coordination and collaboration such that communicating the need to restructure had all but ceased and became fairly automatic!

With Team B, the team structure was less interactive, but was more dictated. Team members were less interested in playing an active role in coordinating the team, but rather focused on their own task. The team leader of this team reacted by dictating the team structure after several attempts at collaborative leading.

Team Communication

There was a significant difference in the amount of team communication for the two teams. Team B had a tense and silent atmosphere for the entire competition, whereas Team A actively communicated and collaborated.

Team A actively attempted to facilitate communication through a variety of methods. The initial attempt was through Internet Relay Chat (IRC). Although this method was never fully realized, Team B never attempted nor reported attempting any virtual communication platform. A possible reason for the failure of the IRC methods is due to all 85 teams in the iCTF sharing the same chat server, and thus creating an insecure place for conversing. Subsequent to the failure of the IRC communication method, Team A resorted to verbal communication throughout the competition. Within this communication, leaders and team members openly discussed what tasks other team members were working on and provided feedback on those tasks when available and appropriate.

If a team member required help on their current task when they hit a roadblock, the team would adjust and facilitate the individual in their task until help was no longer needed. Of the categories of teamwork we watched for, we counted more instances of Team A members verbally asking for, or giving, aid than any other category including planning and role-assigning. In addition, there were several tasks in which even with team help, the task was not completed. As such, the team leaders, with input from the team, often stated that the task should be dropped for another task that was within reach.

Feedback and motivation was higher on Team A than on Team B. After the success of a challenge or exploited system, team members on Team A informed other team members. Often times, this success and announcement of such was then publically congratulated at some level. Occasionally, such congratulations involved the entire team giving accolades to an individual. As the competition progressed, the amount of positive feedback from Team A increased. Team B did not actively congratulate individuals on performance and only had a few moments of congratulations..

Team leader interactions differed between the teams. Team A shared the leadership role among three members. This structure likely supported the resulting behaviors of announcing completed tasks to the team as a whole. One of the team leaders would respond, but it was not always evident at the time which one. This behavior fostered the team atmosphere of sharing any and all information regardless of relevance. Half way through the competition, team leaders started regularly informing the team of the current status of the team including challenges, "money", active services, and current strategies. With some regularity, Team A often became very playful in their interactions.

Although the Team B leader tried to foster a similar atmosphere among Team B, it was never realized. The team leader often went from person to person gathering information on the current status of that individual. Later reported in the focus group, there were instances in which the team leader was unsure of what the team, as a whole, was working on. The leaders of Team A reported that in general they felt as if they knew what the team was doing.

Some of these communication discrepancies could be attributed to cultural and language barriers. Team B contained several members who did not speak throughout the competition. During the focus group, the moderator addressed this issue. The resulting statements concluded that this was in part due to the lack of interactivity of team members. Team A also included an individual with lower interactions than the remainder of the team. However, this individual was occasionally sought out by the team to gather from, and provide to, information regarding the current tasks at hand.

Team Cooperation and Collaboration

In both teams, members relocated and shared computer screens when a member needed help to solve a problem, or when a member had accomplished a task and wanted to show the results of accomplishment. Often, tasks would be given to two or more individuals to work on in collaboration to solve the task. However, the amount of cooperation and collaboration varied by team. Team B members were less inclined to move about with only a subset

of individuals doing so, whereas Team A members often were not found in their own seats.

An important ability Team A established was how to communicate current and completed work. They established a Dropbox folder where people provided written summaries of work when stuck or as they went in order to share relevant information. This allowed higher levels of transactive memory and thus enabled the team to coordinate efforts effectively. This effort supported the already substantial communication by the team. The team was also able to make use of the close proximity within the lab space to pull team members over to talk and ask for help.

Team B tried to utilize a file-sharing tool called "Samba". However, not everyone on Team B knew how to use the system. In contrast to Team A, there was much less effort to find a tool that everyone could use and establish how to communicate and to whom besides the team leader.

It was clear during the focus group that Team A started to develop a sense of how to function as a team whereas Team B felt like they could not develop that sense. The team leader of Team B mentioned his frustration at how stressful it is for a leader to not be able to facilitate team structure. On the other hand, the managers of Team A felt like they had little to manage after a few hours into the competition and that people did their role within the team automatically.

DISCUSSION

In this paper, we observed and documented the performance of two teams competing in the University of California, Santa Barbara's International Capture the Flag contest. There were no obvious differences in experience and expertise that we could identify. Teams were composed of students in a cyber security course. Teams also had similar preparation for the competition with both only having minimal information proceeding the day of competition. Although both teams employed similar strategies, we believe communication made the difference to allow Team A to process information and facilitate a more coordinated performance.

Supporting documentation comes from the winning team of the iCTF. The winning team wrote a follow-up report for the iCTF website in which they talk about the effects of communication and team-level planning (Vienna University of Technology, n.d.). Similar to Team A, they had explicitly worked on strategy and agreed as to how to store files and ask for help. They distributed roles and work in categories, such as the "binary" or "web applications" weeks before the competition began. The instructors monitoring this team evaluated and discussed shortcomings of this team, giving feedback before the competition. Thus the team knew how to communicate and coordinate before the competition began.

These results support that team process is leading to differences in performance for cyber security teams. This could have implications for cyber defense as well. A team of analysts' knowledge and abilities to find patterns will depend on communication efforts between teammates. Prior research shows that cyber defense teams could use help on such processes. Stanard, Thordson, McCloskey and Vincent (2001) found that many analysts within a Network Operations Support Center do not see the potential in coordinating or seeing the larger picture of where their role fits with others. They suggested tools to help coordination and collaborative efforts.

However, there are questions that remain if that implication is true. For example, the structure of a team will change the effects and importance of communication. Lafond, Jobidon, Aube and Trembley (2011) found that communication levels were predictive of performance for teams with more specialized roles (functional teams), but not for teams in which members shared roles (multi-functional teams). For this competition, we did see evidence suggesting that multi-functional teams do benefit from increased communication and collaboration.

The results from this exercise suggest that there are important team-level processes that are associated with higher levels of team performance in a given task. The communication and collaboration from Team A seemed to have helped advance this team in rankings relative to that of the quieter and less collaborative Team B.

FUTURE RESEARCH

Our team is currently developing a synthetic task environment to help capture the influence and role of team process on performance. This environment will use the ground truth and findings from this competition for a more controlled experiment aimed at examining situation awareness, coordination, and other aspects of team process.

ACKNOWLEDGEMENTS

We would like to Dr. Giovanni Vigna for his assistance with the observation of his competition and students. We would also like to thank the students at UCSB. Lastly, we would like to thank Cliff Wang whose insight and information have helped us further our understanding. This work was supported by the Army Research Office under MURI Grant W911NF-09-1-0525.

REFERENCES

Allen, N. J., & Hecht, T. D. (2004). The "romance of teams": Toward an understanding of its psychological underpinnings and implications. *Journal of Occupational and Organizational Psychology*, *77*, 439–461.

Alperovitch, D. (2011). Revealed: Operation Shady RAT. *White Paper*, 1–14. Retrieved from: http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf, on 10/31/2011.

Boe, B., Childers, N., Vigna, G. (2010) Hacking for Fun and Education: Organizing the UCSB iCTF. *Proceedings of the Fifth Annual Graduate Student Workshop on Computing.* October 8, 2010.

Champion, M., Rajivan, P., Cooke, N. J., & Jariwala, S. (2012). Team-Based Cyber Defense Analysis. *2012 IEEE International Multi-Dsiciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support*, March 6-8, New Orleans, LA.

Childers, N., Boe, B., Cavallaro, L., Cavedon, L., Cova, M., Egele, M., & Vigna, G. (2010). Organizing large scale hacking competitions. *Detection of Intrusions and Malware, and Vulnerability Assessment*, 132–152.

Cooke, N. J., Gorman, J., & Winner, J. (2007). Team Cognition. In F. Durso, R. Nickerson, S. Dumais, S. Lewandowsky, & T. Perfect, *Handbook of Applied Cognition, Second Edition* (pp. 239–268). Wiley.

D'Amico, A., Whitley, K., Tesone, D., O'Brien, B., & Roth, E. (2005). Achieving Cyber Defense Situational Awareness: A cognitive task analysis of information assurance analysts. *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting - 2005*, *2005*, 229–233.

De Dreu, C., & Weingart, L. (2003). Task Versus Relationship Conflict, Team Performance, and Team Member Satisfaction: A Meta-Analysis. *Journal of Applied Psychology , 88* (4), 741-749.

Doupé, A., Egele, M., Caillat, B., Stringhini, G., Yakin, G., Zand, A., Cavedon, L., et al. (2011). Hit'em Where it Hurts: A Live Security Exercise on Cyber Situational Awareness. *In 27th Annual Computer Security Applications Conference*. Dec 5-9, 2011.

Entin, E. E. and Serfaty, D. (1999). Adaptive team coordination. Human Factors, 41, 312-325.

Fiore, S. M., Salas, E., Cuevas, H. M., & Bowers, C. A. (2003). Distributed Coordination Space: Toward a Theory of Distributed Team Process and Performance. *Theoretical Issues in Ergonomics Science*, *4*(3-4), 340–364.

Irvine, C. (2011). The Value of Capture-the-Flag Exercises in Education. *Education*, 58–60.

Kraemer, S., Carayon, P., & Duggan, R. (2004). Red Team Performance for Improved Computer Security. *Proceedings of the Human Factors and Ergonomics Society 48th annual meeting* (pp. 1604-1609). Santa Monica: Sage Publications.

Lafond, D., Jobidon, M.-E., Aubé, C., & Tremblay, S. (2011). Evidence of structure-specific teamwork requirements and implications for team design. *Small Group Research. 42,*507–535.

Lewis, K. (2003). Measuring transactive memory systems in the field: Scale development and validation. *Journal of Applied Psychology, 88* (4), 587–604.

Malone, T., & Crowston, K. (1994). The Interdisciplinary Study of Coordination. *ACM Computing Surveys , 26* (1), 87-119.

McCloskey, M., & Stanard, T. (1999). A Red Team Analysis of the Electronic Battlefield: A Cognitive Approach to Understanding How Hackers Work In Groups. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting 1999* (pp. 179-183). Sage Publications.

Stanard, T., Thordson, M., McCloskey, M., & Vincent, P. (2001). *Cognitive Task Analysis and Work-Centered Support System Recommendations for a Deployed Network Operations Support Center (NOSC-D).* Air Force Research Laboratory.

Salas, E., Cooke, N. J., & Rosen, M. (2008). On Teams, Teamwork, and Team Performance: Discoveries and Developments. *Human Factors: The Journal of the Human Factors and Ergonomics Society* , 540-547.

Tremblay, S., Vachin, F., Lafond, D, & Kramer, C. (2012). Dealing with task interruptions in complex dynamic environments: Are two heads better than one? *Human Factors, 54*, 70-83.

Wegner, D. M. (1986). Transactive memory: A contemporary analysis of the group mind. In B.Mullen & G. R. Goethals (Eds.), *Theories of group behavior,* 185- 208. New York: Springer-Verlag.

Vienna University of Technology seclab. (n.d.). *The UCSB iCTF*. Retrieved March 14, 2012, from The UCSB iCTF: http://ictf.cs.ucsb.edu/

UCSB iCTF. (n.d.) UCSB iCTF. Retrieved March 18, 2012, from http://ictf.cs.ucsb.edu.