Software Engineering Institute

Communication Among Incident Responders–A Study

Brett Tjaden
Robert Floodeen

September 2012

TECHNICAL NOTE
CMU/SEI-2012-TN-028

CERT® Program

http://www.sei.cmu.edu

Carnegie Mellon

This material is based upon work funded and supported by the United States Department of Homeland Security under Contract No. FA8721-05-C-0003 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center sponsored by the United States Department of Defense.

Any opinions, findings and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the United States Department of Homeland Security or the United States Department of Defense.

This report was prepared for the

SEI Administrative Agent
AFLCMC/PZE
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

Table of Contents

Abstract **vii**

1 Introduction **1**

1.1 The Participants 1

1.2 Overview 1

2 Tasks **2**

2.1 Task #1: Communicate “Important” Information to Other Teams 2

2.1.1 Description 2

2.1.2 Results and Analysis 3

2.2 Task #2: Identify Phone Numbers and PGP Key IDs for Three Teams 4

2.2.1 Description 4

2.2.2 Results and Analysis 4

2.3 Task #3: Determine If More Teams Prefer Water or Coca-Cola 5

2.3.1 Description 5

2.3.2 Results 6

2.3.3 Analysis 7

2.4 Task #4: Complete Email Message Chain with Other Teams 8

2.4.1 Description 8

2.4.2 Results and Analysis 9

2.5 Task #5: Communicate “Important” Information to Other Teams, One at a Time 9

2.5.1 Description 9

2.5.2 Results and Analysis 10

3 Summary **11**

References **13**

List of Figures

Figure 1: Task #1 Email 2
Figure 2: Task #2 Email 4
Figure 3: Task #3 Email 5
Figure 4: Message Nesting 8
Figure 5: Task #4 Email 9
Figure 6: Task #5 Email 10

List of Tables

Table 1: Time (in Minutes) Messages Were Sent from One Team to Another 3

Table 2: Response Time (in Minutes) for Task #2 4

Table 3: Task #3 Activity 6

Abstract

Responding to some future incident might require significant cooperation by multiple teams or organizations within an incident response community. To study the effectiveness of that cooperation, the Carnegie Mellon® Software Engineering Institute (SEI) conducted a study using a group of volunteer, autonomous incident response organizations. These organizations completed special SEI-designed tasks that required them to work together.

The study identified three factors as likely to help or hinder the cooperation of incident responders: being prepared, being organized, and following incident response best practices. This technical note describes those factors and offers recommendations for implementing each one.

1 Introduction

1.1 The Participants

Participants, who were recruited from an established community of incident response organizations, had to opt in to the study and were assured that their identities would be kept confidential. Although we cannot offer any identifying information about them here for that reason, we can state that participants came from nine organizations in seven European countries. (We hope to use a larger and more diverse group of participants in a future similar study.)

1.2 Overview

We asked the teams to cooperate on one task every two to three weeks. Tasks were designed to take participants 15 minutes or less to complete. Each task was designed to simulate scenarios that might occur during response to an incident. In addition to presenting the teams with different scenarios, we introduced limitations on their communications in order to observe how those restrictions affected completion of the tasks. Each task was fictitious and contained absolutely no sensitive information. We asked teams to carbon (or courtesy) copy (CC) us on all email they sent relating to the tasks so we could monitor their communications and measure various aspects of how they completed the tasks.

2 Tasks

2.1 Task #1: Communicate "Important" Information to Other Teams

2.1.1 Description

Our first task was designed as a baseline to measure how quickly and in what manner teams would disseminate "important" information that other teams might need. In our description of the task, we asked participants to communicate with other teams only via email and provided the names of participating teams but not email addresses, URLs, or any other contact information. It was up to participants to figure out how to find the contact information of the other teams (with whom they might never have communicated in the past). Figure 1 contains the description (with the actual team names redacted) that we emailed to two randomly selected[1] participants to begin the first task.

> *Measuring Incident Response Communication Study Task 1:*
>
> *You have important information that other incident response teams (IRTs) need to know. That important information is the word "Ronaldo."*
>
> *Rules:*
>
> - *If your IRT has already handled this task once, please do not take any further action. You may delete this email and any further copies that you receive.*
> - *If your IRT has not handled this task previously, please forward this email to some other IRT within your community:*
>   - *Please use only email to transmit this message to other IRTs.*
>   - *Please CC the address cert-ir@cert.org in your email.*
>   - *Please contain this exercise to the list of participants identified below.*
>
> *The list of participating teams:*
> *<REDACTED>*

Figure 1: Task #1 Email

[1] We used the random number generator function in MS Excel "rand()" in our tasks.

2.1.2 Results and Analysis

Table 1 shows how many minutes passed between when we sent the initial message and when other messages were sent. We indicate the time when Teams 1 and 3 received our initial message as 0 minutes.

Table 1: Time (in Minutes) Messages Were Sent from One Team to Another

To From	Team #1	Team #2	Team #3	Team #4	Team #5	Team #6	Team #7	Team #8	Team #9	Team Z
Authors	0		0							
Team #1		4	4							
Team #2				61	61					61
Team #3	85	86		72	78		87	71	77	83
Team #4		80			80				80	80
Team #5							101		102	
Team #6			164	164	164					
Team #7		191	191			191				
Team #8				89	89		89			
Team #9										
Team Z						102				

The first thing we noticed was that three different teams did not properly identify team 6 and instead sent the information to team Z, a non-participating incident response organization located in the same country as team 6. After receiving these three messages, team Z helpfully forwarded a copy of the task to team 6 and CC'd our address on the email.

The data indicated that the "important" information was disseminated relatively quickly. It also showed that some teams chose to send it to only two or three other teams, while one team tried to send it to the other eight participating teams (although actually sent it to seven participating teams and team Z).

Furthermore, some teams chose to send a single email message addressed to several other teams, while other participants decided to send individual emails to each of their chosen recipients. One team encrypted and digitally signed the "important" information that it sent to other participants, and another team assigned the task a ticket number.

2.2 Task #2: Identify Phone Numbers and PGP Key IDs for Three Teams

2.2.1 Description

We noticed during the first task that only one team encrypted and digitally signed the email that it sent to other teams. Our second task was designed to measure how quickly and accurately teams could collect vital information about the other participants that would enable them to communicate more securely. We randomly chose three of the nine participating teams and asked all teams to email us the phone number and PGP key ID(s) for those three teams. Figure 2 contains the description (with the actual team names redacted) that we emailed to all participants to begin the second task.

> *Measuring Incident Response Communication Study Task 2:*
>
> *Please find the phone number and PGP key ID(s) for the following three organizations:*
>
> *<REDACTED>*
>
> *When you have collected the information requested, please email it to cert-ir@cert.org.*
>
> *Thank you for your participation.*

Figure 2: Task #2 Email

2.2.2 Results and Analysis

Seven of the nine teams responded quickly to our email, and all seven provided correct answers. Two teams had not responded after five days and were sent reminders. One responded with the correct answers about two hours later, and the other never responded. The table below shows the amount of time (in minutes) each team took to respond.

Table 2: Response Time (in Minutes) for Task #2

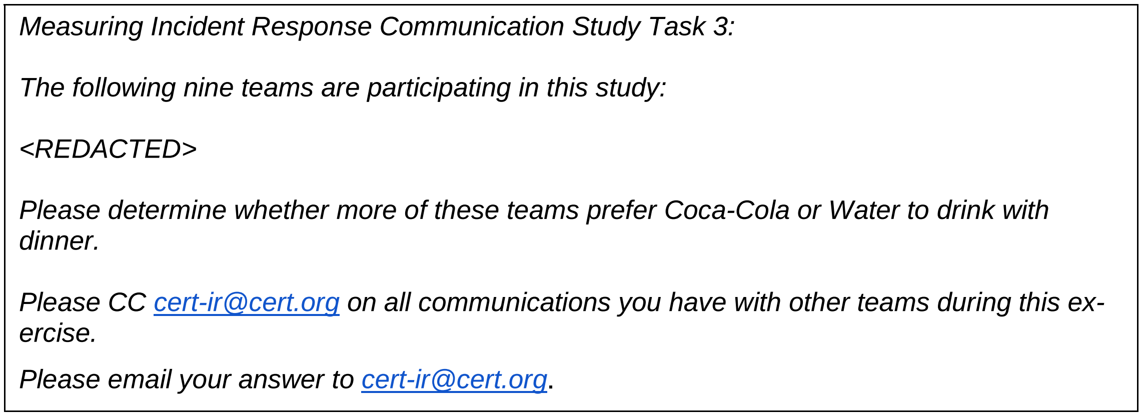
Team	Response Time (in Minutes)
1	84
2	20
3	52
4	------
5	62
6	72
7	7317
8	80
9	36

For this task, three teams digitally signed their messages to us, and one team again assigned our request a ticket number.

2.3 Task #3: Determine If More Teams Prefer Water or Coca-Cola

2.3.1 Description

For our third task, we wanted to examine how teams would handle a task that required distributed agreement. The email we sent to all of them to begin this task is shown in Figure 3.



Measuring Incident Response Communication Study Task 3:

The following nine teams are participating in this study:

<REDACTED>

Please determine whether more of these teams prefer Coca-Cola or Water to drink with dinner.

Please CC cert-ir@cert.org on all communications you have with other teams during this exercise.

Please email your answer to cert-ir@cert.org.

Figure 3: Task #3 Email

We were rather careful in the wording of this message. We did not use the word “vote,” although it is fairly clear that each team needs to express a preference for either water or Coca-Cola. We also did not describe how teams should communicate and tally votes in order to answer our question. Before sending this task out, we wondered how the teams would communicate (would each team send its vote to all other participants?), whether any team would take charge and tally votes, and what would happen if one or more teams did not cast their votes (since we had one team fail to participate in each of the first two tasks).

2.3.2 Results

Table 3: Task #3 Activity

Action	Team	Time	Action	Recipients	Water	Coca-Cola
0	Authors	0	Send out initial email	All	-	-
1	1	123 mins	Vote for water	All	1	0
2	2	173 mins	Vote for Coca-Cola	All	1	1
3	3	176 mins	Vote for water	All	2	1
4	4	254 mins	Vote for Coca-Cola Reported a vote of (2,2)	All	2	2
5	5	290 mins	Vote for water	All	3	2
6	6	373 mins	Vote for water	All	4	2
7	7	398 mins	Vote for water Reported a vote of (5,2)	All	5	2
8	4	26 hours	Declared a winner, water	Authors	5	2
9	7	2 days	Sent email to teams #8 and #9 reminding them to vote	Teams #8 & #9	5	2
10	3	5 days	Reported a vote of (5,2), inquired about teams #8 and #9 (if anyone had heard of them)	All	5	2
11	5	6 days	Reported a vote of (5,2), asked teams #8 and #9 to respond	All	5	2
12	8	6 days 1 hour	Voted for water Reported vote of (6,2)	All	6	2
13	3	6days 1 hour 20 mins	Declared results of (6,2), water being the winner	All	6	2

Each action listed in Table 3 is described in detail below:

1. The first team to take action responded by sending an email to all other eight participants two hours and three minutes after receiving our initial email. That first team notified the other eight teams of its preference for water.
2. Fifty minutes later, another team responded to the first team's email, copied all other teams on the email, and voted for Coca-Cola.
3. Three minutes later, a third team replied to the first team's email, copied all other teams on its email, and voted for water.
4. One hour and eight minutes later, a fourth team replied to the third team's email, copied all other teams on its email, voted for Coca-Cola, and summarized the voting up to that point—listing the two teams that had voted for water and the two that had voted for Coca-Cola.
5. Forty-six minutes later, the fifth team responded to the first team's email, copied all other teams on its email, and voted for water.
6. One hour and twenty-three minutes later, the sixth team responded to the fifth team's email, copied all other teams on its email, and voted for water.
7. Fifteen minutes later, the seventh team responded to our initial email, copied all other teams on its email, voted for water, and summarized the voting up to that point by listing the five teams that had voted for water and the two that had voted for Coca-Cola.

So within six and a half hours of sending out our email, we had votes from seven of the nine participants, and one of the two choices (water) had five of the possible nine votes, meaning it would have the majority of votes no matter how the last two teams voted.

8. Twenty hours then passed with no further communication by any of the teams. At that point, a little over a day after the exercise had begun, one of the teams emailed us announcing the results: five teams for water, two teams for Coca-Cola, and two teams that did not answer.
9. One day later, a different team sent email to the two teams who had not yet responded, included a copy of our initial email, and asked for their votes.
10. About three days later, a third team sent email to all nine participating teams summarizing the vote up to that point and asking if anyone had heard from the two teams that had not responded.
11. The next day, a fourth team sent email to the two teams that had not responded (and copied the other seven teams), summarized the voting to that point, and asked for their votes.
12. Just over one hour later—six days after the task had begun and after inquiries from two other teams—an eighth team responded to one of the inquiries that had been sent, copied all other teams on its email, and voted for water.
13. Twenty minutes later, one of the teams sent email to us announcing the results: six teams for water, two teams for Coca-Cola, and one team that did not answer.

There were no further communications on this task.

2.3.3 Analysis

Eight of the nine teams voted. Only two of the nine teams sent us the answer to our question (whether more of these teams prefer Coca-Cola or water to drink with dinner). We have no doubt that at least eight and possibly nine of the teams knew the answer to our question, but we believe the fact that one team never voted (and we did not specify a deadline) caused some teams to refrain from sending us the results they clearly knew.

Communication was initially ad hoc with early responders simply broadcasting their votes to all participants, but after a while one team decided to summarize all the votes it had seen and add its own to the list. This was probably a good idea, and other teams subsequently adopted that strategy. However, all the teams copied all the other teams on their email: No team took charge of the exercise and offered to collect votes so they would not have to be broadcast to and tallied by all the participants. That was probably acceptable with such a small number of participants, but if there had been more (perhaps 50 or more) this approach would have quickly become unworkable. It would be interesting to try this task with a larger group to discover how quickly teams realize that they cannot all email their votes to everybody and to see how they would work together to solve this problem.

Five of the eight teams that replied assigned the task a ticket number, and four of the eight teams that replied digitally signed their emails. Those digital signatures brought up a possible change for the next iteration of this study: It would be interesting to try this task again, this time introducing forged email messages telling some teams that team X votes for water and telling others that it votes for Coca-Cola. Would all teams agree on which of the two choices got the most votes?

Would teams start disregarding unsigned messages once they started hearing conflicting information on the voting results from other teams?

2.4 Task #4: Complete Email Message Chain with Other Teams

2.4.1 Description

For our fourth task, we wanted to see if the teams could complete a task working serially where each team can complete only part of a task and only after other teams have completed their part. We randomly assigned each team to one of three groups and created nested, encrypted messages.

The idea was to have the task proceed as follows:

Chain 1: Team 1 ➪ Team 2 ➪ Team 3
Chain 2: Team 4 ➪ Team 5 ➪ Team 6
Chain 3: Team 7 ➪ Team 8 ➪ Team 9

We used the message nesting shown in Figure 4. Note that we purposely did not indicate which team was next in the chain: It was up to each team to determine whose public key had been used to encrypt the message and send it to the proper next team.

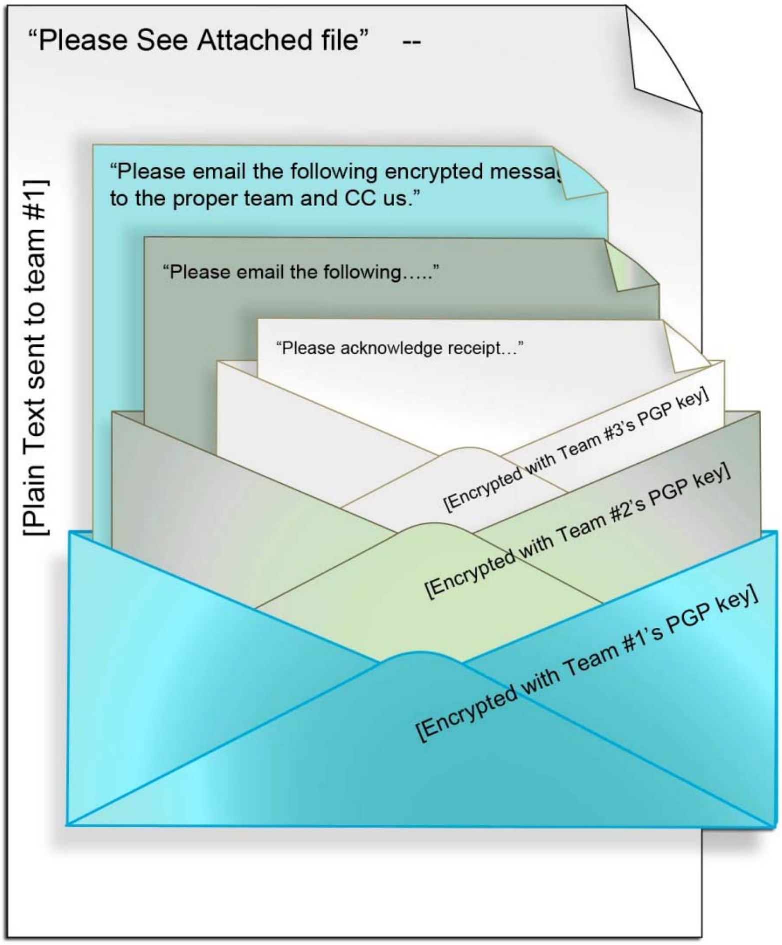
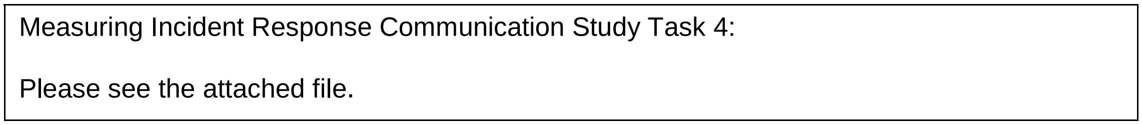

"Please See Attached file" --
[Plain Text sent to team #1]
"Please email the following encrypted messa
to the proper team and CC us."
"Please email the following….."
"Please acknowledge receipt…"
[Encrypted with Team #3's PGP key]
[Encrypted with Team #2's PGP key]
[Encrypted with Team #1's PGP key]

Figure 4: Message Nesting

In these nested messages, the first team could strip off the first layer of encryption and send the result to the second team in the chain. The second team could strip off the next layer of encryption and send the result to the third team in the chain. The third team could strip off the final layer of encryption and notify us that they had received the innermost message. To the first team in each of the three chains, we sent the email message shown in Figure 5 with the encrypted message for the team's chain attached.



Measuring Incident Response Communication Study Task 4:

Please see the attached file.

Figure 5: Task #4 Email

2.4.2 Results and Analysis

The first chain was decrypted and forwarded from the first team in the chain to the second team in the chain 40 minutes after receipt. Twenty-four hours later, the second team had decrypted its part of the message and forwarded the result to the third team in the chain. Twenty-two hours later, the third team acknowledged receipt of the message. It took the three teams just under two days to complete the task.

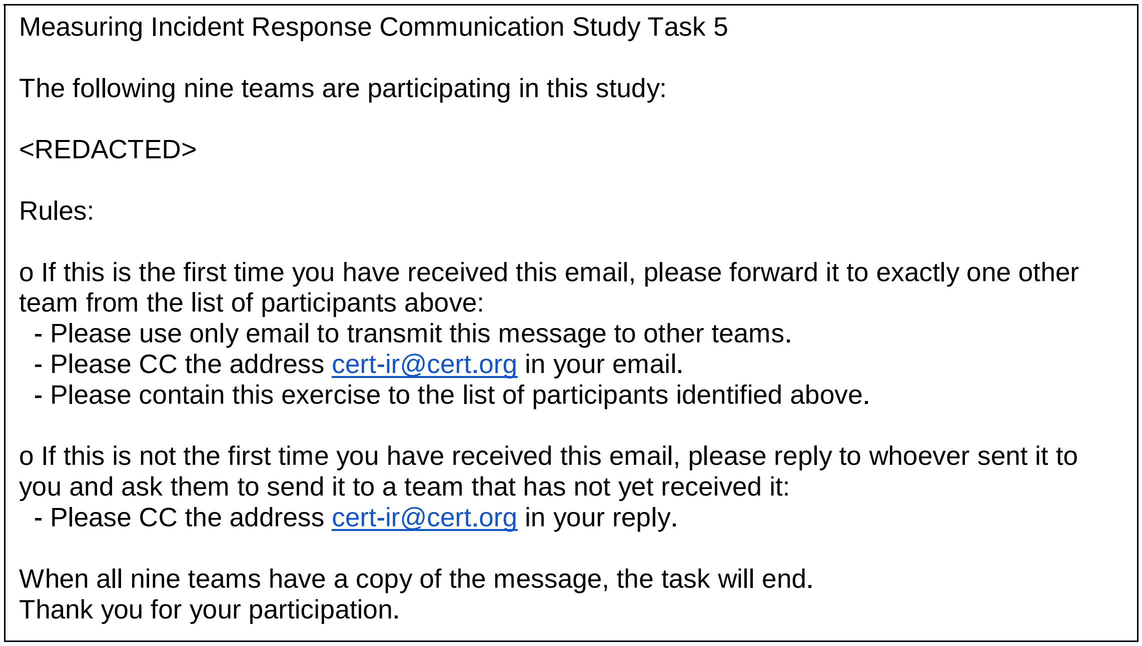
For the second chain, approximately 8 hours after receiving the encrypted message, the first team in the chain forwarded a message to the second team in the chain. Unfortunately, the first team forwarded the original message (still encrypted with the first team's public key). Fifteen and a half hours later, the second team notified the first team of this. Within three minutes, the first team responded to the second team apologizing for the mistake and forwarding the part of the message (encrypted with the second team's public key) that had been revealed when the first team decrypted the message we had sent to it. About 20 minutes later, the second team had decrypted the message it received from the first team and forwarded it to the third team. About an hour and a half later, the third team notified us that it had received and decrypted the last message in the chain. It took just over one day for those three teams to complete the task.

None of the three teams involved in the third chain took any action.

2.5 Task #5: Communicate "Important" Information to Other Teams, One at a Time

2.5.1 Description

For our fifth task, we wanted to redo the first task that involved disseminating information we had designated as "important" to other teams but with a limit on their communication. We told teams that they could only send the information to one other team, and if that team had already received the information, they would have to try another team until they found one that had not yet received it. Early on in the task, we thought it would be very easy for teams to find another team that did not yet have the information. As the task progressed, it would become more and more difficult to find a team that did not yet have the information—unless teams began to track which participants had already received the message. We hoped to see at what point teams would realize this, start keeping a list of who had already participated, and determine a reliable method for managing this information. We selected one team at random and sent it the email shown in Figure 6.



Measuring Incident Response Communication Study Task 5

The following nine teams are participating in this study:

<REDACTED>

Rules:

o If this is the first time you have received this email, please forward it to exactly one other team from the list of participants above:
  - Please use only email to transmit this message to other teams.
  - Please CC the address cert-ir@cert.org in your email.
  - Please contain this exercise to the list of participants identified above.

o If this is not the first time you have received this email, please reply to whoever sent it to you and ask them to send it to a team that has not yet received it:
  - Please CC the address cert-ir@cert.org in your reply.

When all nine teams have a copy of the message, the task will end.
Thank you for your participation.

Figure 6: Task #5 Email

2.5.2 Results and Analysis

We sent the email to a randomly selected team. Seventy-eight minutes later, that team forwarded a copy (not signed or encrypted, and with no evidence of a ticket number) to another participating team. A little over 19 hours later, the second team forwarded the message to a third team. The second team's email was digitally signed and had a ticket number. The third team did not respond. One week later, the second team inquired if their earlier message had been received and again included a copy of the task. The participating team they had selected again failed to respond, and no further action was taken by any of the teams. Unfortunately, the task ended prematurely, and we were unable to observe the team's behavior towards the end as we had hoped.

3 Summary

After observing the teams working on all five tasks, we identified three factors that played a large role in how effectively the teams were able to work together. In our discussion of these factors below, we include recommendations based on the beneficial team behaviors we observed during the exercises.

1. **being prepared**

   Many of the participants in this study had never worked closely before or even communicated with each other, which we felt was a very realistic situation for incident responders who might need to cooperate. Our study highlighted how important it was for teams to be able to locate other organizations and obtain trustworthy information about them (such as their contact information and public keys). We observed one instance of a message being sent to a group that was not even participating in the study because another team mistook it for a team that was. In another instance, a revoked public key was used to encrypt a message for a team because an outdated webpage still listed it as a valid key. To avoid these types of difficulties, we recommend that all incident response organizations complete an RFC 2350 document, publish it in multiple locations, and keep it up to date and consistent everywhere it is published. It is particularly important for information to appear (and appear correctly) on the FIRST[2] and TF-CSIRT[3] websites and the MIT[4] PGP key server.

   Being familiar with the expertise of other organizations and having a general understanding of their activities can also be beneficial. For example, some organizations may know about certain types of attacks or attackers, have access to certain local resources, have the ability to trace an attack back to its origin, or have other specialized skills such as fluency in a specific language. Therefore, through websites or social media, teams should publicize non-sensitive information about their expertise and activities for other incident responders.

2. **being organized**

   In many cases, collaboration and coordination will be improved when participants organize themselves appropriately. Several of our scenarios could have been completed more quickly and easily if some team had stepped forward and offered to coordinate the task or keep a history. Teams should be able to recognize when such coordination would be beneficial and should establish a set of organizational and communication protocols from which to choose. Rules for escalation should also be established as evident in our voting scenario when one team never cast its vote.

   Some teams waited several days, sent the team a reminder, and then gave up when no vote was forthcoming. Other teams noted that there was already a majority regardless of how the last team voted and declared which choice had won immediately. Standards for who should

[2] Forum of Incident Response and Security Teams, http:/www.first.org

[3] Task Force – Computer Security Incident Response Teams, an organization of Terena, http://www.terena.org

[4] Massachusetts Institute of Technology's PGP Key Server, http://pgp.mit.edu/

be included in a task, what roles each participant will play, and the ground rules for participation and completion would have helped in many of our scenarios.

3. **following incident response best practices**
   There was a lot of variation in how the exercises were handled. Some teams always used a ticketing system when presented with a task, some never did, and some used one only at certain times. The teams also handled encrypting and digitally signing communications, or responding to requests from other teams, in very different ways. The following standards recommend that incident response organizations establish and follow standard operating procedures that dictate how incidents (regardless of their apparent importance and severity) will be handled:
   - NIST SP 800-61 revision 2 [NIST 2012]
   - FFIEC InfoBase [FFIEC 2012]
   - ENISA Secure Communication with the CERTs & Other Stakeholders [ENISA 2011]
   - ITIL v3 2011 [OGC 2011, Section 4.2.5.2]

   Some of the more important best practices include always verifying the source and validity of information received; using a ticketing system to manage and track every incident; and digitally signing and, when possible, encrypting all communications. These exercises reaffirmed the importance of these best practices for incident handling.

References

URLs are valid as of the publication date of this document.

[ENISA 2011]
European Network and Information Security Agency (ENISA). *Practical Guide/Roadmap for a Suitable Channel for Secure Communication, Concise Version: Secure Communication with the CERTs & Other Stakeholders.* ENISA, 2011. http://www.enisa.europa.eu/activities/cert/other-work/files/secure-communication

[FFIEC 2012]
Federal Financial Institution Examination Council (FFIEC). *FFIEC IT Examination Handbook InfoBase.* http://ithandbook.ffiec.gov/ (2012).

[NIST 2012]
National Institute of Standards and Technology (NIST). *Computer Security Incident Handling Guide SP 800-61, Revision 2.* NIST, 2012. http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf

[OGC 2011]
Office of Government Commerce (OGC). *ITIL Version 3, Service Operation.* OGC, 2011. http://www.mysarir.com/wp-content/uploads/Books/ITIL_V3_SERVICE_OPERATION.pdf

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503.

1. **AGENCY USE ONLY** (Leave Blank)	2. **REPORT DATE** September 2012	3. **REPORT TYPE AND DATES COVERED** Final

4. **TITLE AND SUBTITLE**

Communication Among Incident Responders–A Study

5. **FUNDING NUMBERS**

FA8721-05-C-0003

6. **AUTHOR(S)**

Brett Tjaden & Robert Floodeen

7. **PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)**

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

8. **PERFORMING ORGANIZATION REPORT NUMBER**

CMU/SEI-2012-TN-028

9. **SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)**

SEI Administrative Agent
AFLCMC/PZE
20 Schilling Circle, Bldg 1305, 3rd floor
Hanscom AFB, MA 01731-2125

10. **SPONSORING/MONITORING AGENCY REPORT NUMBER**

n/a

11. **SUPPLEMENTARY NOTES**

12A **DISTRIBUTION/AVAILABILITY STATEMENT**

Unclassified/Unlimited, DTIC, NTIS

12B **DISTRIBUTION CODE**

13. **ABSTRACT (MAXIMUM 200 WORDS)**

Responding to some future incident might require significant cooperation by multiple teams or organizations within an incident response community. To study the effectiveness of that cooperation, the Carnegie Mellon® Software Engineering Institute (SEI) conducted a study using a group of volunteer, autonomous incident response organizations. These organizations completed special SEI-designed tasks that required them to work together.

The study identified three factors as likely to help or hinder the cooperation of incident responders: being prepared, being organized, and following incident response best practices. This technical note describes those factors and offers recommendations for implementing each one.

14. **SUBJECT TERMS**

Incident response, incident coordination, incident communication

15. **NUMBER OF PAGES**

25

16. **PRICE CODE**

17. **SECURITY CLASSIFICATION OF REPORT** Unclassified	18. **SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	19. **SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	20. **LIMITATION OF ABSTRACT** UL