Communication Among Incident Responders - A Study

Brett Tjaden
Associate Professor
Department of Computer Science
James Madison University
Harrisonburg, VA
Email: tjadenbc@jmu.edu

Robert Floodeen
Member of Technical Staff
CERT Program
Carnegie Mellon University
Pittsburgh, PA
Email: floodeen@cert.org

Executive Summary

For this project, we recruited nine autonomous incident response organizations to help us study how effectively they work together. We asked participants to complete five tasks that we designed and that require cooperation. In this paper, we share some preliminary results of our study in hopes of soliciting feedback.

Overview of the Tasks

The tasks, which used fictitious data, were designed to simulate scenarios that might occur during response to a real incident. As the teams worked on each task, we monitored their communications so that we could measure various aspects of how they completed the tasks. One task dealt with disseminating information we designated as "important", to other teams. Another task asked teams to find contact information for several other participants. The third task required the teams to vote and determine other teams' votes to determine which of the two choices had won. The fourth task used nested, encrypted messages so that each team had to perform decryption, determine the next appropriate team, and forward the result. The fifth exercise again asked teams to disseminate "important" information but restricted the breadth of teams with which they could communicate.

Lessons Learned

1. Be Prepared

Many of the participants in this study had never worked closely or even communicated with each other previously. We view this as a very realistic situation where incident responders might need to cooperate with teams they have not dealt with before. 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 In another instance, a revoked public key was used to encrypt a message for a team because an outdated webpage still listed it as a valid key.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 a RFC 2350 document, publish it in multiple locations, and keep it up to date and consistent everywhere it is published. The FIRST and TF-CSIRT websites and MIT PGP key server are particularly important locations for your information to appear (and appear correctly).

Being familiar with the expertise of other organizations and having a general understanding of their activities can also be beneficial. For example, some organizations 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 make non-sensitive information available about their expertise and activities to other teams.

2. Organize Effectively

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 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. Follow 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 should 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[1]
- FFIEC InfoBase[2]
- ENISA Secure Communication with the CERTs & Other Stakeholders[3]
- ITIL v3 2011[4]

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.

Next Steps

Our next update will detail each of the measurements, the detailed activity involved, our assumptions going into the measurement, lessons learned, and a conclusion of what we think are the most important questions raised by this work.

[1] http://csrc.nist.gov/publications/drafts/800-61-rev2/draft-sp800-61rev2.pdf

[2] http://ithandbook.ffiec.gov/

[3] http://www.enisa.europa.eu/activities/cert/other-work/files/secure-communication

[4] ITIL Service Operation - Incident Management, 4.2.5.2. Incident Logging