Detecting, Analyzing and Responding to Security Incidents: A Qualitative Analysis

Rodrigo Werlinger David Botta

University of British Columbia, Vancouver, Canada
{rodrigow,botta@ece.ubc.ca}

ABSTRACT

This study develops categories of responses to security incidents, based on a grounded theory analysis of interviews with security practitioners, with a focus on the tasks performed during security incidents, and the necessary resources to perform these tasks. The results include a list of types of incidents, a model for the tasks, the skills employed, and the strategies used during security incidents. A security incident can be understood in terms of three stages: detection, analysis, and response. Each stage is comprised by tasks that are performed using different skills, strategies, and resources. We also recommend that development of security tools focus on: correlation of multiple sources of information, including the activities of different projects in distributed environments; and better trade-off between portability and visualization.

Categories and Subject Descriptors

K.6.5 [**Management of Computing and Information Systems**]: Security and Protection

General Terms

Security Incident

Keywords

Security Tasks, Resources

1. INTRODUCTION

Persistence and cost are the two factors that have motivated several studies about better practices for dealing with security incidents [10, 9]. Nevertheless, the literature is sparse investigating IT professionals who have to deal with security incidents, in terms of which tasks they actually perform and which resources they need to handle the complex scenarios given by real incidents [1]. This lack of research makes it difficult to evaluate and improve the support that IT security professionals need to respond efficiently to security incidents.

This study investigates how security practitioners deal with security incidents. To do so, this study adopted an empirical focus, using ethnographic techniques [14] — questionnaires and interviews — to capture security practitioners' perspectives during security incidents.

Results include (1) the tasks performed by security practitioners during security incidents, and (2) the skills and tools necessary to deal with security incidents. The task model shows that the process of dealing with security incidents can be separated in three stages: detection, analysis and response. To perform these tasks, three skills are used by practitioners: pattern recognition, generation of hypothesis, and collaboration. Knowledge about the IT infrastructure, protocols and attack patterns are also used during security incidents. Tools used by the participants comprised various applications ranging from general IT to specific security tools to home made scripts.

Results also include that strategies to deal with security incidents are required resources. Strategies of isolation and simulation were mentioned as a way to find out the source of the incident and verify the existence of malicious software respectively.

The rest of the paper is organized as follows. The next section discusses related work. Section 3 describes the methodology, including data collection and analysis. Section 4 reports the results. Section 5 analyzes the results. Conclusions and future work are in Section 6.

2. RELATED WORK

Barrett et al. [12] used ethnographic methods to study systems administrators. They used several quantitative and qualitative methods to gather information from IT administrators in large industrial service delivery centers. With 101 preliminary surveys, 12 interviews (sysadmins, managers, team leads, and others in various roles), 6 case studies (at 4 industrial service delivery centers), a log diary kept by a system administrator for 10 months (2002-2003), and observations of the tasks of 12 system administrators (over 25 days), they give several recommendations about developing tools to effectively support system administrators' tasks. Although Barrett et al.'s findings touch a broad spectrum of IT administration (e.g., database, web server, operating system), nothing is mentioned about specific practices, tasks and needs of administration in the domain of IT security. In addition, they are more focused on tool development, rather than providing models of the tasks performed by their par-

Workshop on Usable IT Security Management (USM '07), July 18, 2007, Pittsburgh, PA, USA.

ticipants.

Kandogan and Haber [1] aimed at evaluating security administration tools in real environments. They spent 40 days performing an ethnographic study of security administrators from a University in USA. Based on some real situations faced by these security administrators, they give recommendations about future developments of IT security tools. Neither Barrett et al. nor Kandogan and Haber provide models of the tasks and resources related to the participants. In contrast, my paper not only aims at providing recommendations about improvements on tools and resources used by security practitioners, but also obtains a deeper understanding of the task space and complexities during security incidents.

3. METHODOLOGY

The approach used in this study is based on ethnographic techniques. The use of ethnography [14] makes it possible to study security practitioners in the context of security incidents within their organizations. The ethnographic data were analyzed using grounded theory [4].

The ethical approval for contacting participants, the recruiting process, the interviews themselves and their transcriptions, were managed in the context of the HOT Admin project [3]. This project's field work provided 24 questionnaires and 14 interviews of IT security professionals with responsibilities in IT security. The data were analyzed using grounded theory [4]. The profile of the participants and their organizations is described in the next section.

3.1 Data Sources

The 14 interviews from HOT Admin field study comprised the main source of data for this study: thirteen of them mentioned IT incidents or IT security incidents (this study discarded one interview that focused on physical security). The interviews were accompanied by a questionnaire submitted by the participants, with general information about their responsibilities and technical background. All the interviewees came from British Columbia, and most of them (12) were from academic organizations.

Academic organizations have been the focus of other similar studies [1, 11]. The main reason for taking participants from academic organizations is they are easier to recruit than from other organizations. Recruitment is a serious issue in IT security studies, as shown in [13].

3.2 Data Analysis

The analysis started with selecting data that pertains to security incidents. A security incident was considered as: "any real or suspected adverse event in relation to the security of computer systems or computer networks " [2]. The aspects of security that were used to materialize this definition were confidentiality, integrity and availability [7].

About 13 situations related to security incidents were identified. This information was coded in an iterative process, starting with open coding and continuing with axial and theoretical coding [4]. At this stage, two models were generated. The first one comprised the tasks that the participants performed during security incidents. The second one accounted for the tasks in terms of resources (skills, knowledge and tools) necessary to deal with these incidents.

The posterior analysis was based on further elaboration of the "memos" [4] written during the coding process, which were initially used to draft any idea, comment or interesting finding from the data.

4. RESULTS

4.1 List of Security Incidents

The open-ended interview questions did not explicitly ask about security incidents. Nevertheless, every participant talked about security incidents. Table 1 lists the types of incidents mentioned by the participants. This classification takes into account the source of the incident, rather than its consequences.

The most common incidents reported were related to malicious software. Within this type of incident, our participants distinguished between specific types of malicious software (trojan, malware, worm), the quantity of compromised machines, the type of asset compromised (user's PC or internal Host), and the regularity of the event.

Incidents related to Human Resources were mentioned in terms of the violation of internal policies. These violations were related with improper use of the organization's resources. These incidents were also characterized by the sensitivity of the internal communications during their investigations.

Phishing was a type of incident mentioned by one of the two participants in the private sector. As this incident had particular characteristics different from the other incidents, it was classified in another category.

Suspected security incidents include those incidents that either were being investigated and there was no clarity about their causes, or those incidents that could materialize serious compromises in the future. In the former case, two of the participants reported situations where the source of the problem was not clear, and they had to speculate about the presence of a malicious source. One of them specified: *"So we try to put a proxy in between —a very powerful Linux machine— and then it started crashing. So like I said: I don't think it's malicious, it's all firewalled away."*

These incidents were interesting because the participants needed to perform more tasks and use more resources and skills to discover the source of the problem.

4.2 Tasks

Table 2 shows the main tasks performed by our participants during the security incidents. These tasks were grouped in three main stages: detection, analysis and response. These stages account for the temporal sequence[1] since a security incident is "perceived" by the security practitioner until a concrete action to stop it is taken. In between, during the analysis, security practitioners have to perform several tasks to confirm the incident, assess its scope, and find out the source of the problem or the attack. Below, the main tasks from the detection and analysis stages are described. Secondary tasks are omitted for space reasons.

Monitor systems and networks: The objective of this kind of task was to detect incidents by either direct inspection of systems and networks, or by using SW tools that detect anomalies in the systems' behavior. This kind of task was common for all types of incidents.

Receive notifications: This kind of task was also common for all types of incidents. Some notifications came from

[1]a detailed sequence analysis is omitted here

Table 1: List of security incidents

Description	Incidents
Malicious SW	1. Host infected with a worm 2. A user's PC with Malicious Software 3. Large outbreak of virus 4. A Host with a Trojan
Human Resources	5. Download porn 6. Hack other systems using organization's infrastructure 7. Send threats emails from organization's servers
Phishing	8. One case of phishing reported by a client
Suspected incidents	9. Peaks of traffic 10. Unreachable systems 11. Devices crashing 12. Network slow 13. Port scanning

Table 2: List of tasks performed during a security incident

Stage	Task
Detection	Monitor systems or networks Receive notifications
Analysis	Verification Assess the incident Track the source of the attack Collect more data to find the source of the problem Interact with other specialists Generate action plan Evaluate legal implications
Response	Turn off ports or services Clean-up systems Re-initialize services Patch or reconfigure systems System's restoration Administrative sanctions

third parties external to the organizations, as the participant who dealt with the phishing attack explained *"...we had a person, not even a member of any of our organizations or customers, who emailed our privacy office."*

Verification: Verification of important information in the incident follows detection of the incident. The main objective of this kind of task was to confirm, often with alternate data sources and file types, that the information from the detection stage (either from notification or monitoring) was accurate and there was effectively a compromise (i.e. not a false positive). To do this, participants either checked directly with the people responsible for the suspected machine, or used log files from other systems and tools to perform their own analysis.

Assess the incident: The primary objective of this kind of task was to evaluate the incident, in terms of its magnitude and possible consequences. Usually, our participants performed this task while they were performing the verification process.

Track the source of the attack: The participants rapidly recognized some incidents as attacks. In this case, just after the notification, the participants started tracing the originator of the malicious activity. For example, in the case of the phishing, the participant used the information from the e-mail that notified about the phishing attack to find where the web page that impersonated the web page of his organization was hosted.

Collect more data to find the source of the problem: Some incidents required more data to analyze and find the source of the problem. This type of situation occurred when the data from monitoring the systems showed patterns that were (1) not recognized by our participants, and (2) were insufficient to explain the anomaly. Incidents that included this task were considered "suspected security incidents", because malicious sources could not be ruled out.

Interact with other specialists: Most of the tasks listed required that our participants interact with other specialists in some way. Sometimes this interaction was part of preestablished procedures that required contacting other specialists to perform tasks. Other times these interactions were less formal and our participants had to cooperate *ad-hoc* with other stakeholders to, for example, complete information about the incident, or to come up with specific plans of action or to investigate.

4.3 Resources

4.3.1 Tools

A recurrent example of tools was the use of Shell/Perl scripts written by the same security practitioners. These scripts started looking for specific patterns of suspicious activity in firewalls and IDSs' log files. Then, they generated automatic e-mails to those responsible for handling the incidents.

There were also specialized tools to monitor virus activity. Two participants said they used McAfee EPO to get reports of quantity of viruses per machine. To analyze the packets of the network and find out the source of the attack or the problem, tools like TCPDump and Ethereal were used. In this case, a participant had to not only know how to use these tools, but also to have knowledge about filtering techniques to reduce and extract those parts of the files that were useful for the investigation.

4.3.2 Skills

Pattern recognition: Especially during the detection stage, our participants frequently performed pattern recognition. Examples are: set a predefined threshold in the number of e-mails per machine to detect suspicious activity; recognize the characteristic patterns of DOS attacks; recognize IRChat in some human-readable layers (colored blue by Ethereal) of TCPDump.

Hypothesis generation: When the cause of a problem is not clear, hypotheses about the incident may be required. To illustrate, one participant described a case of unexplained spikes of traffic in the network: *"we haven't been able to trace what the spike is due to...We think that there has been a breakdown in TCP/IP connections between our router and our server."*

Cooperation: Our participants had to cooperate and communicate with others for different reasons: make a more efficient investigation; execute specific actions in-situ; gather

network information; interact with other specialists who had experienced similar problems or incidents; design a response plan to clean-up systems infected by a virus, etc.

4.3.3 Strategies

Isolation: Isolation was a strategy used to either verify incidents or to find out what was causing the anomaly or the attack. For example, one participant who was investigating why the internet connection was slow stated: *"...based on traffic utilization on the network, where it was coming from...we finally isolated — hey, its that new firewall that we just brought up."*

Simulation: To investigate security incidents, participants sometimes needed to simulate the compromise, either in a controlled environment or in the production network. In the interviews, these simulations had the objective to either verify the existence of malicious software in a compromise, or get more evidence and clues about the the source of the incident.

5. DISCUSSION

5.1 What to expect from a security incident

One important result from the analysis is that a security incident can be separated into three stages: detection, analysis and response. Each one has its own tasks and resources, and accounts for the temporal sequence of events, since the incident or suspected incident is *perceived* until a concrete action is taken.

The results showed no strong correlation between the security training specified in the questionnaire and the specific tasks performed or resources used by the security practitioners. Only in the case of the phishing attack, was training explicitly highlighted as an asset to respond to that type of incident.

Another aspect to consider in handling security incidents is the way that people interact and the different roles involved. There was no incident in which the same person performed all the tasks from detection to response.

5.2 Better security tools

Our preliminary analysis showed that there are several opportunities to improve IT security tools. For example: (1) tools that correlate other sources of information, such as a project's inventories, with the results of monitoring networks and systems, would help to discard false positives in highly distributed environments; (2) use different types of files as inputs an outputs to make tools more flexible and usable in situations where time and bandwidth are constraints to transmit and charge large files; and (3) utilize visualization features to indicate flows and meaning of network traffic.

A tool with such features could be used to analyze log files from different sources, and to make the meaning of the data more readily apparent.

6. CONCLUSIONS AND FUTURE WORK

Our categories of responses to security incidents are well-grounded in empirical evidence, and provide a reasonable basis for future research. Our results include a list of types of security incidents, a model for the tasks, the skills employed, and the strategies used during security incidents. We gained some insight into the stages of response to a security incident, the high-level interactions between different people during an incident, and issues around which to improve security tools.

Future research is expected to bolster and refine our understanding of the deployment of tasks with respect to different kinds of security incident. We expect to fill out our map of how the skills, strategies and distribution of responsibilities come into play over the sequence of tasks.

7. REFERENCES

[1] Eser Kandogan and Eben M. Haber, "Security Administration Tools and Practices", Security Administration tools and practices, O'Reilly, August 2005, chapter 18, ISBN: 0-596-00827-9.

[2] Computer Emergency Response Team (CERT): Computer Security Incident Response Team (CSIRT) main page (2007), available at: http://www.cert.org/csirts (accesed February 2007)

[3] HOT Admin project (2007), available at: http://www.hotadmin.org (accesed February 2007)

[4] Kathy Charmaz, "Constructing Grounded Theory", SAGE publications, 2006.

[5] Bagchi, K. and G. Udo, "An Analysis of the Growth of Computer and Internet Security Breaches", Communications of the AIS, 2003. 12(46): p. 684-700.

[6] Gordon, Lawrence A., Loeb, Martin P., Lucyshyn William and Robert Richardson, CSI/FBI Computer Crime and Security Survey, 2006, available at: http://www.gocsi.com/ (accesed February 2007)

[7] Wikipedia, CIA triad web page definition (2007), available at: http://en.wikipedia.org/wiki/CIA_triad (accesed April 2007)

[8] The Fifth Workshop on the Economics of Information Security (WEIS 2006): Main Page (2007), available at: http://weis2006.econinfosec.org/ (accesed February 2007)

[9] TCP/IP Network administration: chapter 12. Network Security (2007), available at: http://www.unix.org.ua/orelly/networking/tcpip/ch12_01.htm (accesed February 2007)

[10] Forum for Incident Response and Security Teams: Main Page (2007), available at: http://www.first.org/ (accesed February 2007)

[11] Sherri Davido and Bob Mahoney, "Incident Response and Large Event Handling in the Research University", 16th Annual FIRST Conference on Computer Security Incident Handling, Budapest, Hungary, June 2004.

[12] Barrett, R. and Haber, E. and Kandogan, E. and Maglio, P. and Prabaker, M. and Takayama, L., "Field studies of computer system administrators: Analysis of system management tools and practices", Proceedings of the Conference on Computer Supported Collaborative Work, 2004.

[13] Andrew G. Kotulica, Jan Guynes Clark, "Why there aren't more information security research studies", Information & Management 41 (2004) 597607.

[14] Fetterman, David M., "Ethnography, Step by Step", Applied Social Research Methods Series, Volume 17, second edition, 1998.