Received 30 September 2009
Accepted 1 October 2009

Preparation, detection, and analysis: the diagnostic work of IT security incident response

Rodrigo Werlinger
University of British Columbia, Vancouver, Canada
Kasia Muldner
School of Computing and Informatics, Arizona State University, Tempe, Arizona, USA, and
Kirstie Hawkey and Konstantin Beznosov
University of British Columbia, Vancouver, Canada

Abstract

Purpose – The purpose of this paper is to examine security incident response practices of information technology (IT) security practitioners as a diagnostic work process, including the preparation phase, detection, and analysis of anomalies.

Design/methodology/approach – The data set consisted of 16 semi-structured interviews with IT security practitioners from seven organizational types (e.g. academic, government, and private). The interviews were analyzed using qualitative description with constant comparison and inductive analysis of the data to analyze diagnostic work during security incident response.

Findings – The analysis shows that security incident response is a highly collaborative activity, which may involve practitioners developing their own tools to perform specific tasks. The results also show that diagnosis during incident response is complicated by practitioners' need to rely on tacit knowledge, as well as usability issues with security tools.

Research limitations/implications – Owing to the nature of semi-structured interviews, not all participants discussed security incident response at the same level of detail. More data are required to generalize and refine the findings.

Originality/value – The contribution of the work is twofold. First, using empirical data, the paper analyzes and describes the tasks, skills, strategies, and tools that security practitioners use to diagnose security incidents. The findings enhance the research community's understanding of the diagnostic work during security incident response. Second, the paper identifies opportunities for future research directions related to improving security tools.

Keywords Diagnostic testing, Data security, Data analysis

Paper type Research paper

1. Introduction

Diagnostic work, i.e. the practice of noticing and categorizing problems, as well as defining the scope of remediation, is a pervasive feature of Information Technology

The authors would like to thank the participants for taking part in the study, members of the Laboratory for Education and Research in Secure Systems Engineering (LERSSE) for feedback on earlier versions of this paper, and the anonymous reviewers of the paper for their valuable comments. This work has been supported by the Canadian NSERC Strategic Partnership Program, Grant STPGP 322192-05.

Information Management &
Computer Security
Vol. 18 No. 1, 2010
pp. 26-42
© Emerald Group Publishing Limited
0968-5227
DOI 10.1108/09685221011035241

Security Management (ITSM). Diagnosis is particularly prevalent during security incident response, one of the primary responsibilities of security practitioners (Botta *et al.*, 2007; Kandogan and Haber, 2005). Despite its prominence as an activity, the field of security incident response is still in its infancy (Killcrece *et al.*, 2005). In fact, based on a retrospective comparison of the 1998 internet worm incident with the state of IT security in 2003, Spafford (2003) concludes that several security-related aspects worsened during that time. In particular, Spafford highlights that the security community has been unable to learn the importance of communication during incident response. He proposes that the security community should find better ways to not only coordinate during incidents, but also to distribute incident-related information. While a number of organizations provide guidelines for the incident response process (e.g. Computer Emergency Response Team (CERT) and National Institute of Standards and Technology (NIST)), there are few empirical investigations on how security practitioners respond to incidents (for exceptions, see, for instance (Goodall *et al.*, 2004a; Riden, 2006)). The research presented in this paper aims to fill this gap.

Our results extend the findings of Werlinger *et al.* (2009), who identify nine activities that require security practitioners to interact with other stakeholders, one of which is security incident response. We extend those results by:

- analyzing security incident response from a broader perspective, rather than focusing only on interactions; and
- identifying the diagnostic aspects during interactions involved in the preparation, detection, and investigation phases of security incidents.

The contribution of our work is twofold. First, using empirical data, we analyze and describe the tasks, skills, strategies, and tools that security practitioners use to diagnose security incidents (Section 4). Our findings enhance the research community's understanding of the diagnostic work during security incident response. Second, we identify opportunities for future research directions related to improving security tools (Section 5). For instance, our analysis shows that regardless of how advanced a security tool is for supporting diagnostic work, practitioners must still customize that tool to fit the specific needs of their organization. Today's tools, however, provide very little if any support for this customization process. Before explaining our study methodology (Section 3), we present the related work.

2. Related work

Given the challenges of managing security incidents, a number of guidelines (Casey, 2002; Stephenson, 2004) and associations (e.g. CERT and NIST) exist that provide support for the incident response process. Recently, Mitropoulos *et al.* (2006) synthesized the information from the various standards and existing research to propose a general incident response management framework. While these various efforts may provide some support for the incident response process, Bailey *et al.* (2007) discuss how best practices and formal standards for IT work tend to be either so high level that they provide little guidance on work practices, or so low level that they are inflexible to rapid changes in the technology and organization.

One of the tools designed to support practitioners during the detection of security incidents is an intrusion detection system (IDS). Goodall *et al.* (2004b) and Thompson *et al.* (2006) rely on data from nine and two semi-structured interviews, respectively, to identify the phases of intrusion detection work. Goodall *et al.* (2004b) suggest that intrusion detection is challenging due to the need for analysts to coordinate with other stakeholders and the need for high expertise, both technical and organizational. Werlinger *et al.* (2008) analyze data from nine interviews to identify security practitioners' perceptions of the advantages and disadvantages of IDSs. They also analyze data from participatory observation to show that IDS usability is hindered by lack of technical resources and ITSM's distributed nature.

Some research focuses on descriptive case studies of real-life examples related to security incidents. Casey (2005) presents a case study of an intrusion against one organization and stresses the role of collaboration during incident diagnosis and containment. Gibson (2001) describes a denial of service attack on his company. The diagnosis of the incident included both technical troubleshooting as well as interaction with various parties. Riden (2006) describes a series of security incidents on a large academic network. Key factors contributing to the incidents included ineffective communication and collaboration between the organization's security professionals, which led to inconsistent preventative measures and untimely notification of vulnerabilities. Schultz (2007) describes a variety of sources of information that had to be combined in order to diagnose an incident in one organization. While these case studies can provide useful data, they only involve a single organization, and do not rely on formal evaluation methodologies to collect and analyze the data. As far as we are aware, the only formal studies that exist investigate a small subset of security incident response, namely a specific tool used to detect security incidents (an IDS), as described above.

We can also draw from research of diagnostic work within other types of organizations. Orr (1986) investigates the diagnostic process for copier repair to show that story telling is used both as a cooperative diagnostic activity and to provide organizational knowledge of interesting cases. Yamauchi *et al.* (2003) describe the problem-solving practices of service repair technicians. Their findings illustrate that technicians rarely follow instructions from existing documentation, but rather glean the required information from a variety of sources such as colleagues, systems, and informal documents.

3. Methodology

We framed our study with the following research questions:

RQ1. How do security practitioners perform diagnostic work when responding to security incidents?

RQ2. What tools do security practitioners need to perform this type of diagnostic work?

RQ3. How can such tools be improved to better support security practitioners?

Table I summarizes information on the 16 participants who did discuss diagnostic work and whose data we considered for the analysis presented here. For presentation purposes, we identify our interview participants according to their interview number (i.e. I1, . . . , I39).

To answer our research questions, we analyzed our interview data corpus from the HOT Admin project; see Hawkey *et al.* (2008) for an overview of other themes of analysis. HOT Admin researchers have conducted 39 semi-structured *in situ*

Table I. Participant information

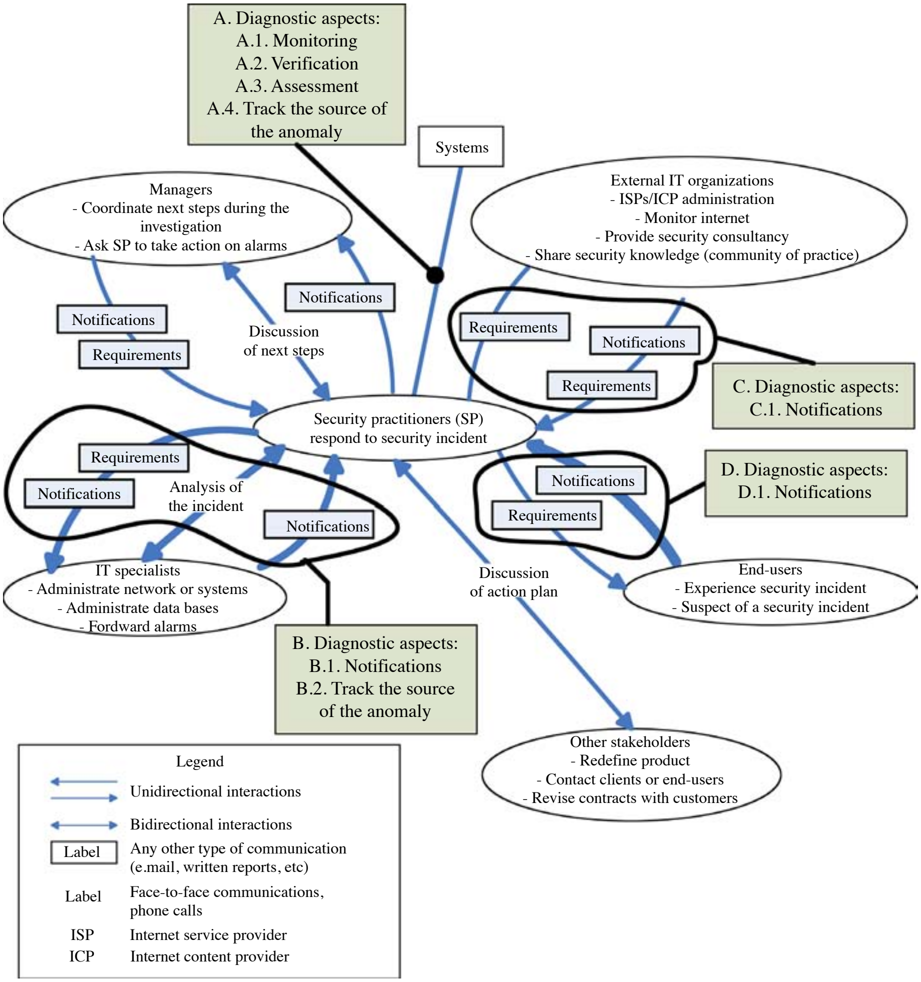
Organization type	Position type Security manager	Security specialist	IT practitioner with security tasks	Total
Academic (3)	I2	I3, I9, I11, I24	I7, I8, I22	8
Financial services (1)	–	I4	–	1
Scientific services (1)	–	–	I12, I13	2
Manufacturing (1)	–	I21	–	1
Telecommunications (1)	–	I32	–	1
IT consulting firm (1)	–	–	I26	1
Insurance (1)	I38	I39	–	2
Total	2	8	6	16

interviews with security practitioners, who worked for a variety of organizations (11 different organizations from seven sectors). Participants were asked a variety of security-related questions (e.g. ITSM challenges, ITSM tasks and tools, organizational influences, and to name a few). Each interview lasted approximately one hour and was subsequently transcribed and sanitized to preserve the participants' anonymity. As is typically the case with semi-structured interviews, not all participants were asked the same questions, and not all discussed topics relevant to our research questions on diagnostic work during security incident response.

We used qualitative description (Sandelowski, 2000) to analyze our data, as follows. First, we analyzed the interview transcriptions to identify excerpts pertaining to diagnostic work, focusing on work related to security incidents. We used CERT's definition of a security incident: "any real or suspected adverse event in relation to the security of computer systems or computer networks" (Killcrece *et al.*, 2003). Second, we organized the excerpts into different stories or "memos" (Charmaz, 2006) describing how security practitioners perform diagnostic work and the key challenges they face during this process.

4. Results

Before we present our results, we provide an overview of the diagnostic process during security incident response (see Figure 1 (A, B, C, and D), adapted from Werlinger *et al.* (2009)). Although not illustrated in the diagram, the diagnostic process begins with a preparation phase, which includes knowledge gathering about vulnerabilities and risks and configuration of tools (e.g. IDS). Each incident begins with the detection of an anomaly in an organization's IT systems (e.g. users experiencing slow access to internet). During this process, our participants performed two types of activities: monitoring (Figure 1, A.1) and sending and receiving notifications (Figure 1, B.1 and C.1). Monitoring involves intensive use of IT tools (e.g. IDSs and antivirus) and also requires a high degree of expertise to identify patterns of anomalous activity in the networks. Such knowledge is often tacit, in that people are unaware of possessing it and/or how it could be valuable to others; furthermore, tacit knowledge is not easily shared (Polanyi, 1966). Notification involves extensive collaboration with other stakeholders, who are either directly monitoring systems or indirectly receiving notifications from other stakeholders. After noticing an anomaly in the IT


A. Diagnostic aspects:
A.1. Monitoring
A.2. Verification
A.3. Assessment
A.4. Track the source of the anomaly
Systems
Managers
- Coordinate next steps during the investigation
- Ask SP to take action on alarms
External IT organizations
- ISPs/ICP administration
- Monitor internet
- Provide security consultancy
- Share security knowledge (community of practice)
Notifications
Notifications
Requirements
Discussion of next steps
Requirements
Notifications
Requirements
C. Diagnostic aspects:
C.1. Notifications
Security practitioners (SP) respond to security incident
Requirements
Notifications
Analysis of the incident
Notifications
Notifications
Requirements
D. Diagnostic aspects:
D.1. Notifications
IT specialists
- Administrate network or systems
- Administrate data bases
- Fordward alarms
Discussion of action plan
End-users
- Experience security incident
- Suspect of a security incident
B. Diagnostic aspects:
B.1. Notifications
B.2. Track the source of the anomaly
Other stakeholders
- Redefine product
- Contact clients or end-users
- Revise contracts with customers
Legend
Unidirectional interactions
Bidirectional interactions
Label
Any other type of communication (e.mail, written reports, etc)
Label
Face-to-face communications, phone calls
ISP
Internet service provider
ICP
Internet content provider

Notes: Thicker arrows indicate more frequent collaboration; diagnostic aspects are highlighted (A, B, C, and D)

Figure 1.
Collaboration among stakeholders during security incident response

infrastructure, participants moved to analysis of the anomaly. This stage included diagnostic tasks such as: verification (Figure 1, A.2), assessment (Figure 1, A.3), and tracking the source of the anomaly (Figure 1, A.4 and B.2). To perform these tasks, our participants required effective:

- communication skills to collaborate with other stakeholders; and
- analytical skills to generate hypothesis about the causes of the anomaly.

When the cause of the anomaly was found, participants moved to containing the incident. We now describe these activities.

4.1 Preparation phase

In preparation of monitoring systems in an effort to detect security incidents, security practitioners perform tasks such as vulnerability assessments of their IT systems and configuration of their monitoring tools. For brevity, the discussion of the configuration process of monitoring tools has been integrated within Section 4.2.

Vulnerability assessment. Our participants used scanners such as Nessus, and/or ISS to determine if IT systems were susceptible to known vulnerabilities; lists of vulnerabilities were obtained from public servers maintained by the IT security community. To use the security scanners effectively, our participants needed to be highly familiar with configuration of their organization's networks, in order to specify the systems to be scanned. Failure to provide accurate information could result in, for example, the tools scanning other organization's networks (I9), who might interpret such unexpected scanning activity as preparation for an attack.

Further complicating the usage of the scanners was lack of accuracy. Participant (I32) described how scanner output needed to be corroborated to:

- discard false positives; and
- adjust the scanners' interpretation of vulnerability severity.

To discard false positives, this participant had to directly access the scanned systems and verify each of the vulnerabilities identified by the scanner, by checking the corresponding processes and applications. If the scanner information was accurate (i.e. a vulnerability), then the participant still needed to confirm the scanner's assessment of the vulnerability's severity, relying on his tacit knowledge of the IT infrastructure to do so. To illustrate, the scanner could report a critical vulnerability, with an accompanying recommendation (e.g. the installation of a security patch), but a security practitioner could assess the severity differently. This occurred, for instance, when the scanner labeled an application as highly vulnerable, but that application was running on a network protected by a firewall. Of course, this does not mean that the vulnerability did not exist, but that the priorities suggested by the scanner had to be adjusted, so that resources could be allocated to mitigate more critical vulnerabilities.

4.2 Detection of an anomaly

During the process of detecting an anomaly in an organization's IT systems, our participants performed two types of activities: monitoring their organization's IT systems with a variety of tools (Figure 1, A.1) and sending and receiving notifications (Figure 1, B.1 and C.1). In order to effectively detect an anomaly, participants required tacit knowledge about the organizations' IT systems and services. For example, one participant (I3) knew that end-users in his organization typically generate less than 50 e-mails per day, and so a higher number of e-mails signaled a potential anomaly.

Monitoring tools. Examples of the tools included antivirus software and IDSs. Antivirus software was used to detect viruses and to generate reports about virus activity in the infrastructure (I3, I4, I12, and I24). IDSs were used to "sniff" network traffic to find matches with the signatures of known attacks. A number of challenges hindered monitoring tools' effective usage, both during tool installation during the preparation phase and during actual operation.

Werlinger *et al.* (2008) illustrated in-depth five challenges of installing and configuring an IDS, which we summarize here. First, to install an IDS and interpret its output, security practitioners must have extensive knowledge of the type of network traffic that is allowed within their organization. Unfortunately, this information is rarely explicitly documented and difficult to obtain. A second challenge relates to the fact that it is sometimes necessary to involve external stakeholders, complicating communication. For instance, in the case of IDS installation, a vendor's input was required to verify that its server was not blocking IDS traffic, who did not know anything about the target organizational networks. Third, IDSs are embedded into actual production networks that must continue to be operational, complicating the troubleshooting process when issues arise during installation. A fifth challenge is a lack of usability; for instance, during the IDS installation, diagnosis of issues was complicated by misleading and uninformative error messages.

During active monitoring with an IDS, some of our participants (I4, I9, I12, and I24) found it very challenging to generate meaningful reports on monitoring outcomes, largely due to the overwhelming amount of false positives generated. To reduce false-positives, an IDS needs to be customized to fit a given organization's characteristics, a time-consuming and difficult process that some of our participants preferred to avoid (I3, I4, I9, I24, and I12). Other monitoring tools were less complex than IDSs, although these tools also suffered from usability issues. For example, SmokePing was used to identify when systems were up or down (I13). This tool minimized false positives, and its output was easy to interpret. The tool, however, also had a disadvantage, namely that the alarms it generated did not include any information on the cause of the problem.

The monitored traffic's characteristics also limited the usability of security tools. For instance, encrypted traffic created a constraint; without access to encrypted data, participants had limited options to detect malicious code in the packets (I36). High-volume traffic made it impossible to monitor some network areas (I3 and I24). In these cases, participants had to select specific networks to monitor, based not only on the capacity of the security tools but also on historical network data, i.e. where the most critical incidents occurred in the past (I37). Another way to target specific networks is through vulnerability assessment (as described in the preparation phase).

As the above examples demonstrate, tools for monitoring typically have pros and cons. In some instances, security practitioners combined tools in unique ways to maximize their utility, a practice known as bricolage. For instance, one participant (I12) combined two tools (TCPDump and Ethereal) to generate and analyze, respectively, the log files he needed. He alternated between the advantages of portability (TCPDump) and good visualization (Ethereal):

> [TCPDump provides] common analysis format [...] it's also a portable format [...] it [Ethereal] shows the SYN and RESET in one color and then the PUSH commands in another color. So it is obvious there is content in there.

Owing to usability issues and budget constraints, our participants often resorted to creating their own tools to detect anomalies in the IT infrastructure (I2, I3, I8, I9, I12, I22, and I24). These tools were scripts, programs for the command interpreter of an operating system. One participant (I3) noted that scripts relieved the burden of manually analyzing raw log files. To create effective scripts, participants needed both technical expertise and knowledge about the IT infrastructure within their organization. For example, one participant (I3) could list the network addresses of the computers with suspiciously high number of e-mails; this allowed him to selectively monitor some systems more than others. The same participant developed a script to generate only one alarm upon detection of abnormal traffic, to avoid having vast volumes of alarms associated with the same anomaly. Another participant (I2) explained how he used scripts to detect denial of service attacks, and to notify the appropriate administrators, alleviating the burden of a practitioner having to deal with the notification (Figure 1, B.1).

Notifications. The complexity of IT systems and the lack of resources to actively monitor all systems meant that our participants relied on notifications as a passive method of detecting security incidents (Figure 1, B.1 and C.1). Our participants received notifications from various stakeholders, including IT professionals and end-users. Often, these notifications required communication among stakeholders. For example, participant I12 described how an external organization (MyNetWatchman) had detected malicious traffic generated from one of the systems he administered (Figure 1, C.1). He received this notification from another colleague (Figure 1, B.1) who was notified by MyNetWatchman. This chain of notifications among different security practitioners was also mentioned by a participant who was involved in a response to a phishing attack (I4): "we had a person, not even a member of any of our organizations or customers, who emailed our privacy office [. . .] then the privacy office contacted me directly" (Figure 1, C.1). Another participant (I38) received notifications from his organization's problem management system. Our participants also received notifications about incidents from end-users (Figure 1, D.1), in the form of complaints that the internet access was blocked (I11 and I22). In one organization, Microsoft's monthly patch release day was treated as notification of a security incident to initiate coordination with the relevant stakeholders (I38).

4.3 Analysis of an anomaly

Once a potential anomaly was detected, practitioners investigated it further, which comprised at least three tasks: verification (Figure 1, A.2), assessment (Figure 1, A.3) and tracking the source of the anomaly (Figure 1, A.4 and B.2).

Anomaly verification. During anomaly verification, participants tried to confirm, often with alternate data sources, that a compromise actually occurred. One (I3) described this verification:

> I always try and verify by a second or third source. So [I would] go back to the Argus [IDS] [. . .] check the Argus logs and see what's actually happened; [. . .] then I would go to one of my other logs; what have I seen in the logs of the Windows box; was that a real compromise or not.

Verification may also require collaboration with external organizations. One participant (I20) was investigating traffic from an external server that was generating malicious traffic to his organization. With the external organization's consent, he used *nmap* to determine the ports that the server had open. This showed him that the server had been compromised, which led him to access the server to check its internal status. Another (I28) performed similar steps when dealing with a server that was generating high quantities of traffic to the internet.

When participants had access to machines that stakeholders reported infected by malicious software, they did not necessarily need tools to confirm the infection. One (I26) used his experience to identify patterns that indicated the machine had malicious software (e.g. "funny" icons or processes running). He also explained how his experience taught him to run the tools to remove the malicious software at least twice. Another (I28) indicated how during verification, he relied on his experience to know what type of connection pattern was normal from one server to another:

> This is based on experience [. . .] we consider [it] is normal [connections] from one public IP address [to] all websites. But if IP address goes to every port of the IP address and it is a website then this is not normal.

Anomaly assessment. If an incident was indeed confirmed, during its assessment, security practitioners estimated the incident's magnitude and consequences (I3, I4, and I39). In some organizations, the policy is for the potential cost of the incident to the organization to be communicated to managers who will make a determination of whether to proceed; however, one participant (I38) described how some incidents that did not meet the organization's criteria for high risk may still be investigated by the security team in order to protect their systems. One participant (I3) described the assessment process and how it shaped the next steps:

> I might go through the logs to see what kind of traffic I'm getting from this IP address – is it scans? is it a successful compromise? So it depends on what I find, depends on what I do.

Another (I14) described assessing a phishing attack by checking how many e-mails were sent from the organization's e-mail server.

Tracking the anomaly source. In this step, participants aimed to determine the source of the incident. Two (I9 and I12) used their knowledge about hacking patterns to diagnose the source of an anomaly related to malicious software. One (I9) mentioned that diagnosing denial of service attacks was straightforward and could be accomplished by inspecting the volumes of specific network traffic: "denial of services are easy to spot, cause it's sending mil lions of the same thing actually over and over and over again, with very little iteration." Another participant (I12) identified hacking activity by looking for specific type of traffic:

> [. . .] there is some content here and it looks like IRC [Internet Relay Chat]. So I figure that this is somebody controlling it, the machine [. . .] [IRC is] very popular with hackers as a control mechanism.

Participants also relied on their technical knowledge to perform forensic tasks on compromised servers. If the source of an incident was due to the actions of an internal employee, stakeholders within human resources may be contacted (I39).

When the source of an incident was difficult to diagnose, participants found it especially helpful to interact with other specialists, particularly ones who could offer a novel perspective as they were new to the investigation or had a different background. As an illustration, participant I13 had to investigate an incident related to loss of service from the organization's IT systems. He decided to check the systems *in situ,* and asked for help from another specialist, "because two eyes are better than one." However, the hardware looked normal, and they decided to involve another specialist in the analysis. She thought that the problem was with a small network switch that had not been checked during an earlier inspection; they reset the switch and the network recovered. Another participant (I11) described needing help from a specialist in a different department to trace the flow of traffic in an under-performing network. Through this collaboration, they were able to isolate the device that was slowing traffic:

> We also contacted IT services [to] see if they could see, based on traffic utilization on the network, where it was coming from [. . .] we finally isolated – hey, it's that new firewall that we brought up.

In one organization, recent security incidents are discussed weekly so that security practitioners can learn about the current threats and help brainstorm the resolution of challenging incidents (I39).

In addition to collaboration, another strategy participants used to identify the cause of an incident involved simulation of the incident. One participant (I13) mentioned how he was collecting information from actual situations where he repeated the conditions of failure: "So we try to put a proxy in between [. . .] and then it started crashing [. . .] [but] as soon as we put in no filtering [. . .] bad things stop happening." In another case, a participant (I12) wanted more specific information about the type of malicious traffic that was causing anomalies. He explained how he downloaded the same suspected malicious software to provide such information: "It's saying [. . .] downloading a tool from some website. Okay, so I do that, download this tool and run it through the antivirus and it says okay, this is some dial-up."

Some of the security incidents we described were solved during the analysis process. In other instances, incident containment was necessary. This was accomplished in various ways, including: by turning off ports or services in external organizations (I4) and by cleaning up IT systems by reinstalling software (I9).

5. Discussion

Our analysis shows that response to security incidents requires intensive diagnostic work. We first summarize how this occurs before discussing how technology can be improved to better support diagnostic tasks performed by security practitioners.

5.1 How security practitioners diagnose security incidents

As we summarize in Table II, during the diagnosis of security incidents our participants performed several tasks that relied on various security tools, and five key skills: pattern recognition, hypothesis generation, communication, bricolage (i.e. dynamic integration of security tools in novel, unanticipated ways (Botta *et al.*, 2007)), and tacit knowledge about their organizations and IT systems.

Both ITSM in general and diagnostic work during ITSM in particular are fairly new fields; as such, researchers can borrow insights from more mature fields. We illustrate this with a discussion of the anomaly detection phase. To isolate the source of the anomaly, our participants complemented the use of skills with the application of two strategies: collaboration and simulation. As far as collaboration is concerned, diagnostic work involved dynamic groups of IT specialists to evaluate the different situations and isolate the source of an incident. This strategy of involving various specialists during diagnosis is also employed in "high reliability organizations" (HROs), such as electric and nuclear power plants (Weick and Sutcliffe, 2001). These organizations are highly interactive, complex, and tightly coupled, that is, changes in one part of the organization imply changes in other parts. When safety incidents occur in these organizations, different teams are dynamically formed depending on the type of incident. Once the incident is resolved, these *ad hoc* groups are dissolved and do not leave a trace of their existence in the formal structure of their organization. More research is needed to understand how the diagnosis of security incidents might

Stage	Task	Skills and strategies	Security tools
Preparation	Vulnerability assessment	Tacit knowledge	Scanners Community lists
	Tool Configuration	Tacit knowledge Communication	Complex tools that must be configured to the organization (e.g. IDS)
Anomaly detection	Monitoring	Tacit knowledge Pattern recognition Collaboration Simulation	Scripts IDS
	Receiving notifications	Tacit knowledge Communication	Incident ticketing system
Anomaly analysis	Verification	Tacit knowledge Hypothesis generation	Scripts
	Assessment	Tacit knowledge Pattern recognition	Applications to administer IT systems (e.g. fire wall management system)
	Tracking the anomaly source	Pattern recognition Hypothesis generation Communication Bricolage	Anti-virus

Table II.
Summary of tasks, skills, and tools used during the diagnostic work of security incident response

be improved by adopting strategies used during the investigation of safety incidents in HROs, such as safety incident procedures in nuclear reactors, as shown in Park and Jung (2003).

As far as simulation is concerned, this strategy is used extensively in the field of medicine to help students learn to diagnose disease (Roy *et al.*, 2006). Appropriate training is an important issue for ITSM (Rayford *et al.*, 2001), but as far as we are aware simulation is not used during ITSM training. Thus, it would be interesting to investigate if and how IT security could borrow from the field of medicine to rely on simulation not only during security incident response, but also during training.

5.2 Opportunities for improving IT security technology

Security incident response is a multi-faceted activity, where the corresponding diagnosis requires a mix of both strong technical and communication skills. Our participants faced many challenges when diagnosing security-related problems. At least some of these challenges stemmed from insufficient tool support caused by usability issues (e.g. unhelpful or uninformative error messages). Our study identified a number of other aspects of insufficient tool support. We now offer suggestions on research directions and guidelines for improving security tools, grounding our discussion in both our participants' experiences and related work.

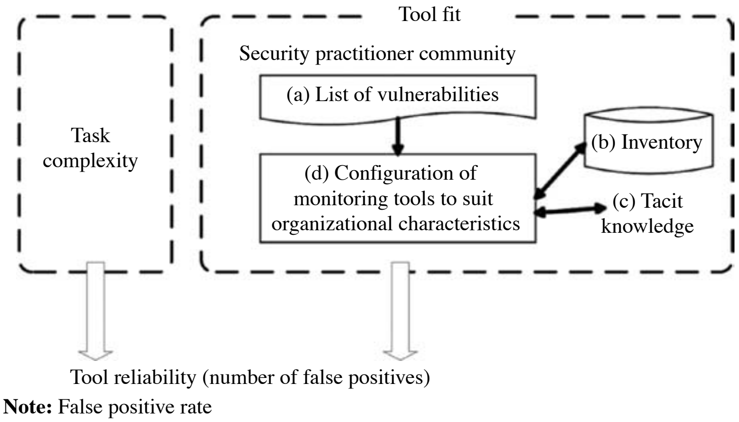
Task complexity. A key challenge our participants mentioned pertained to security tools that monitored IT systems and generated alarms upon detection of anomalous events. These monitoring tools generated overwhelming numbers of false positives (i.e. alarms that corresponded to innocuous events), which placed a high burden on security practitioners who had to investigate the alarms. Our analysis suggests that task complexity influences tool reliability, and furthermore, that there is a tradeoff between the complexity of the task supported by a tool and the tool's reliability:

the more complex the task, the less reliable the tool's output for that task. For example, IDS tools perform a variety of complex tasks; these tools generated many more false positives and so required more intervention from practitioners than SmokePing, a simple tool that only checked system availability. On the other hand, SmokePing's simplicity was not without disadvantages: its basic functionality meant that it did not provide information about incidents unrelated to the availability of systems (e.g. attacks to guess the users' passwords).

The above discussion highlights that the tradeoff between task complexity and tool reliability is a dimension that must be taken into account during tool evaluation. In particular, more research is needed to understand the pros and cons of security tools designed to perform complex tasks, as compared to tools that are intended for simple tasks. A second dimension that needs to be taken into account when evaluating tools is support for tool integration, as we describe shortly. First, however, we present a second factor influencing monitoring tool reliability.

Customization to ensure tool fit. A practitioners' ability to configure a monitoring tool to a given organization's characteristics directly impacts the number of false positives produced by that tool (Figure 2, right). Recall that in the preparation phase, which included configuration of monitoring tools, practitioners relied on generic lists of attacks and vulnerabilities (Figure 2(a)). These lists are maintained by security practitioners around the world and are available on public servers (e.g. lists.sourceforge.net). Although the lists provide a good starting point and highlight the collaborative nature of ITSM, they correspond to huge quantities of generic data, making the customization task difficult for security practitioners. Lack of adequate tools and/or customization support also meant that our participants had to develop their own tools to perform tasks related to the diagnosis of security incidents. This illustrates how difficult it is to develop standard security tools that fit every organization's needs for the diagnosis of security incidents. Botta *et al.* (2007) propose that security tools have to support tailorability, so that practitioners can customize tools via their own scripts.

The above discussion illustrates that regardless how advanced a security tool is, ITSM diagnostic work still requires customization of the tool to the specific reality of a given organization (Figure 2(d)). The customization often requires access to a complete


Tool fit
Security practitioner community
(a) List of vulnerabilities
(b) Inventory
Task complexity
(d) Configuration of monitoring tools to suit organizational characteristics
(c) Tacit knowledge
Tool reliability (number of false positives)

Note: False positive rate

Figure 2.
Forces influencing tool reliability

inventory of an organization's IT systems (Figure 2(b)). Such an inventory is very costly to create and maintain, given the challenges of ITSM (Gagne *et al.*, 2008). For instance, the dynamic nature of the IT environment forces systems to be constantly upgraded and/or replaced, requiring practitioners to continually update the system inventory. In general, to improve the efficiency of diagnostic ITSM work, more research is needed to investigate how to optimize the process of customizing a generic list of vulnerabilities. One option is to use Artificial Intelligence techniques, so that tools automatically adapt a generic vulnerability list to a given organization's characteristic, as is done in so-called anomaly based IDSs.

Customization also requires intensive use of both knowledge that is usually not shared among practitioners and not explicitly documented (Figure 2(c)). Gagne *et al.* (2008) suggest that it is necessary to provide support for transforming security practitioners' knowledge needed during tool configuration into explicit knowledge that can be shared with others. One way in which this could occur is through support for customizable scripts. In addition to increasing the usability of a tool through the facilitation of customization, such support has a second benefit: the scripts capture practitioners' tacit knowledge. This benefit was also noted by Halverson *et al.* (2004), who suggested that supporting the practice of bricolage (discussed next) can aid in the capture and transformation of knowledge within an organization.

Tool integration. Depending on the diagnostic work performed, our practitioners used scripts either as stand-alone tools or in combination with other tools via bricolage, i.e. the re-use of existing tools in new and unanticipated ways. Halverson *et al.* (2004), who studied the trouble-shooting process at a helpdesk, discuss how the practice of bricolage for tools and processes is inherent to group work. Botta *et al.* (2007) show that ITSM work in general involves bricolage, and our results illustrate how this skill is also practiced during diagnosis of security incident incidents. Note that bricolage is a special instance of vendor-designed tool integration.

How tools should be developed to support bricolage is an open question. Novel evaluation methodologies may be needed as there has been little study of how tool integration in general and bricolage in particular impact tool usability. Halverson *et al.* (2004) suggest that the practice of bricolage allows for reuse of expertise with the existing tools. However, integration must be considered in conjunction with task complexity, since the latter also impacts tool usability. To illustrate, bricolage support may be beneficial across the board, from simple to complex tasks; alternatively, bricolage could place high cognitive load on practitioners, making it only beneficial for complex tasks. We need to develop a richer understanding of the ways in which tools are used during diagnostic work when responding to security incidents; this understanding can support the specification of the complex scenarios in which these security tools should be evaluated (Redish, 2007).

Verification of incidents via data correlation. To diagnose security incidents, our participants had to correlate different sources of information. To do so, they not only had to understand how various IT systems were related, but also needed security tools that were able to process and relate information from these different sources. To satisfy this need, security tools need to process information from a variety of sources with different formats and structure. For instance, a tool developed by Cisco, a major vendor of network devices and monitoring tools, can integrate with different tools to correlate information and generate consolidated reports.

In the same vein, security tools that integrate data need to process very large data volumes, which in turn must be reified in a meaningful way. Unfortunately, our participants found the on-line reports needed during diagnosis different to generate. To deal with this limitation, one option is to abstract the tasks of data synthesis and visualization away from the standard security tools towards specialized tools that only focus on these tasks. Abstraction has the advantage of providing a separation of functionality, i.e. raw data collection vs data processing. This in turn provides flexibility to plug in a variety of devices into the specialized reification tools.

Multi-faceted simulation support. As we described above, diagnostic work during security incidents involves security practitioners performing simulations to verify or investigate an anomaly. Complicating simulation work is that in some instances, it needs to be performed in production systems that needed to remain operational. To address this issue, Fisler *et al.* (2005) describes an approach for a specific type of simulation involving access control rules. Along a similar vein, Chiasson *et al.* (2007) propose that any security-system changes should be easily reversible; this guideline ensures that any simulation-introduced problem in a production system is easily reversed. Our results show that diagnostic work during security incident response requires practitioners to perform simulations in distributed systems administered by various practitioners, and so requires collaboration. Since collaboration complicates the simulation process, we propose that tool support for simulation need to address not only the technical factors, but also include functionality that supports collaboration between different IT practitioners as they track the simulations and evaluate their consequences.

6. Conclusion

Our qualitative analysis illustrated the preparation, detection and analysis phases of diagnostic work during security incident response. This important process required active collaboration among our participants and other stakeholders. Participants used different technologies to support their tasks, developing their own tools when they did not have the required security tools for specific tasks. In our discussion, we offer several recommendations to improve security tools support for diagnostic work during responses to security incidents. These recommendations include criteria for evaluating usability of security tools in complex scenarios. Further research is needed to expand and refine our understanding on how technology can best provide the required support to security practitioners when they respond to security incidents.

References

Bailey, J., Kandogan, E., Haber, E. and Maglio, P. (2007), “Activity-based management of it service delivery”, *CHIMIT ’07: Proceedings of Symposium on Computer Human Interaction for the Management of Information Technology, Cambridge, MA*, pp. 1-5.

Botta, D., Werlinger, R., Gagne, A., Beznosov, B., Iverson, L., Fels, S. and Fisher, B. (2007), “Towards understanding IT security professionals and their tools”, *Proceedings of Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA*, pp. 100-11.

Casey, E. (2002), “Error uncertainty and loss in digital evidence”, *International Journal of Digital Evidence*, Vol. 1 No. 2.

Casey, E. (2005), “Case study: network intrusion investigation – lessons in forensic preparation”, *Digital Investigation*, Vol. 2 No. 4, pp. 254-60.

Charmaz, K. (2006), *Constructing Grounded Theory*, Sage, London.

Chiasson, S., van Oorschot, P.C. and Biddle, R. (2007), "Even experts deserve usable security: design guidelines for security management systems", *SOUPS 2007 Workshop on Usable IT Security Management (USM), Pittsburgh, PA*, pp. 1-4.

Fisler, K., Krishnamurthi, S., Meyerovich, L.A. and Tschantz, M.C. (2005), "Verification and change-impact analysis of access-control policies", *ICSE '05: Proceedings of 27th International Conference on Software Engineering, St Louis, MO*, pp. 196-205.

Gagne, A., Muldner, K. and Beznosov, K. (2008), "Identifying differences between security and other IT professionals: a qualitative analysis", *Proceedings of HAISA'08: Human Aspects of Information Security and Assurance, Plymouth*, pp. 69-80.

Gibson, S. (2001), "The strange tale of the denial of service attacks on GRC.com", available at: http://whitepapers.zdnet.co.uk/

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004a), "I know my network: collaboration and expertise in intrusion detection", *CSCW '04: Proceedings of ACM Conference on Computer Supported Cooperative Work (CSCW), New York, NY*, pp. 342-5.

Goodall, J.R., Lutters, W.G. and Komlodi, A. (2004b), "The work of intrusion detection: rethinking the role of security analysts", *Proceedings of Americas Conference on Information Systems (AMCIS), New York, NY*, pp. 1421-7.

Halverson, C.A., Erickson, T. and Ackerman, M.S. (2004), "Behind the help desk: evolution of a knowledge management system in a large organization", *CSCW '04: Proceedings of ACM Conference on Computer Supported Cooperative Work (CSCW), New York, NY*, pp. 304-13.

Hawkey, K., Botta, D., Werlinger, R., Muldner, K., Gagne, A. and Beznosov, K. (2008), "Human, organizational, and technological factors of IT security", *Ext. Abstracts of ACM Conference on Human Factors in Computing Systems (CHI 2008), Florence*, pp. 3639-44.

Kandogan, E. and Haber, E.M. (2005), "Security administration tools and practices", in Cranor, L.F. and Garfinkel, S. (Eds), *Security and Usability: Designing Secure Systems that People Can Use*, O'Reilly, Sebastopol, CA, pp. 357-78.

Killcrece, G., Kossakowski, K., Ruefle, R. and Zajicek, M. (2003), "State of the practice of computer security incident response teams (CSIRTs)", available at: www.cert.org/archive/pdf/03tr001.pdf

Killcrece, G., Kossakowski, K., Ruefle, R. and Zajicek, M. (2005), "Incident management", Technical Report, US Department of Homeland Security, Washington, DC.

Mitropoulos, S., Patsos, D. and Douligeris, C. (2006), "On incident handling and response: a state of the art approach", *Computers and Security*, Vol. 25 No. 5, pp. 351-70.

Orr, J.E. (1986), "Narratives at work: story telling as cooperative diagnostic activity", *CSCW '86: Proceedings of ACM Conference on Computer-Supported Cooperative Work (CSCW), New York, NY*, pp. 62-72.

Park, J. and Jung, W. (2003), "The requisite characteristics for diagnosis procedures based on the empirical findings of the operators' behavior under emergency situations", *Reliability Engineering & System Safety*, Vol. 81 No. 2, pp. 197-213.

Polanyi, M. (1966), *The Tacit Dimension*, Doubleday, New York, NY.

Rayford, R.H., Vaughn, B. Jr and Fox, K. (2001), "An empirical study of industrial security engineering practices", *The Journal of Systems and Software*, Vol. 61, pp. 225-32.

Redish, J. (2007), "Expanding usability testing to evaluate complex systems", *Journal of Usability Studies*, Vol. 2 No. 3, pp. 102-11.

Riden, J. (2006), "Responding to security incidents on a large academic network", available at: www.infosecwriters.com/text_resources/

Roy, M.J., Sticha, D.L., Kraus, P.L. and Olsen, D.E. (2006), "Simulation and virtual reality in medical education and therapy: a protocol", *Cyber Psychology and Behavior*, Vol. 9 No. 2, pp. 245-7.

Sandelowski, M. (2000), "Whatever happened to qualitative description?", *Research in Nursing & Health*, Vol. 23 No. 4, pp. 334-40.

Schultz, E.E. (2007), "Computer forensics challenges in responding to incidents in real life setting", *Computer Fraud & Security*, Vol. 12, pp. 12-16.

Spafford, E.H. (2003), "A failure to learn from the past", *Annual Computer Security Applications Conference (ACSAC), Las Vegas, NV, December 8-12*, pp. 217-33.

Stephenson, P. (2004), "The application of formal methods to root cause analysis of digital incidents", *International Journal of Digital Evidence*, Vol. 3 No. 1.

Thompson, R.S., Rantanen, E. and Yurcik, W. (2006), "Network intrusion detection cognitive task analysis: textual and visual tool usage and recommendations", *Proceedings of Human Factors and Ergonomics Society Annual Meeting (HFES), Santa Monica, CA*, pp. 669-73.

Weick, K. and Sutcliffe, K. (2001), *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, CA.

Werlinger, R., Hawkey, K., Botta, D. and Beznosov, K. (2009), "Security practitioners in context: their activities and interactions with other stakeholders within organizations", *International Journal of Human Computer Studies*, Vol. 67 No. 7, pp. 584-606.

Werlinger, R., Hawkey, K., Muldner, K., Jaferian, P. and Beznosov, K. (2008), "The challenges of using an intrusion detection system: is it worth the effort?", *Proceedings of Symposium on Usable Privacy and Security (SOUPS), Pittsburgh, PA*, pp. 107-16.

Yamauchi, Y., Whalen, J. and Bobrow, D.G. (2003), "Information use of service technicians in difficult cases", *CHI '03: Proceedings of Human Factors in Computing Systems, Fort Lauderdale, FL, April 5-10*, pp. 81-8.

About the authors

Rodrigo Werlinger (CISSP) received a degree in Electrical Engineering from the University of Chile and an MASc degree in Electrical and Computer Engineering from the University of British Columbia, Vancouver, Canada in 2008. He has work experience in IT security in the telecommunications sector, having designed and implemented IT security for telecommunication services from 2002 to 2006. At the time this work was conducted, he was a Research Assistant in the Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca), working on the HOT Admin project.

Kasia Muldner is a Post-Doctoral fellow at Arizona State University, in the Computer Science division of the School of Computing, Informatics and Decision Systems Engineering. She obtained her PhD in the Department of Computer Science at UBC, under the supervision of Dr Cristina Conati in the Laboratory for Computational Intelligence. Her research interests span human-computer-interaction, including usable security, as well as artificial intelligence and cognitive science.

Kirstie Hawkey is an NSERC Post-Doctoral Research Fellow with appointments in both the Department of Electrical and Computer Engineering and the Department of Computer Science at the University of British Columbia. She received her PhD in Computer Science from Dalhousie University in 2007. Her research interests include usable privacy and security and personal information management, particularly within the context of group work and assistive technologies. She is a Member of the ACM and IEEE.

Konstantin Beznosov is an Assistant Professor in the Department of Electrical and Computer Engineering, University of British Columbia, where he founded and directs the Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca). His primary research interests are distributed systems security, usable security, secure software engineering, and access control. Prior to coming to UBC, he was a Security Architect with Quadrasis, Hitachi Computer Products (America), Inc., he did his PhD research on engineering access control for distributed enterprise applications at the Florida International University. Konstantin Beznosov is the corresponding author and can be contacted at: beznosov@ece.ubc.ca