Security Administrators: A Breed Apart

Eben M. Haber, Eser Kandogan
IBM Almaden Research Center
650 Harry Road
San Jose, CA 95120
+1 408 927-1224
{ehaber,eser}@us.ibm.com

ABSTRACT
System administrators (sysadmins) are the linchpin of civilization, managing the Information Technology (IT) infrastructures on which modern life depends. Unfortunately, there has been a lack of research on sysadmin practices and consequently admin tools are often not designed to support their tasks effectively. Over the past five years, we conducted a series of field studies investigating the work practices and environments of admins managing several types of systems and infrastructures. We found that sysadmins are notably different from typical computer users in several dimensions. We also observed considerable variance among sysadmin specialties. Especially interesting are security administrators (secadmins), who act as detectives and intelligence agents to ensure that IT resources are used appropriately, preparing for and responding to attacks by human antagonists. In this paper we profile security administration work by analyzing tasks, tools, and practices in comparison to other system administration specialties. Our data suggests that the human element is a primary factor shaping the problems, environment, and work practices of security administration.

Categories and Subject Descriptors
H.5.2 [User Interfaces]: user-centered design, K.6.4 [Systems Management], K.6.5 [Security and Protection].

General Terms
Management, Security, Human Factors.

Keywords
Ethnography, System Administration, Security Administration.

1. INTRODUCTION
System administrators (sysadmins) are a crucial yet often overlooked group. Without their diligent work deploying, configuring, maintaining, and troubleshooting Information Technology (IT) infrastructures, much of modern business, government, and communication would come to a stand-still. Unfortunately, there has been a lack of published research on system administration and consequently administration tools are often not well aligned to sysadmin work practices and environments. Over the past five years, we conducted a series of field studies investigating the work practices and environments of administrators managing operating systems, website infrastructures, databases, storage, security, and data center operations. Common to all these specialties, we found a number of characteristics that set sysadmins apart from other computer users. We also observed considerable variance among sysadmin specialties. Security administrators (secadmins) are particularly interesting with their role as part detective and part intelligence agent: they must ensure that IT resources are used appropriately, preparing for and responding to attacks by human antagonists. In this paper we profile security administration work by analyzing tasks, tools, and practices, comparing security practices and environments to those of other system administration specialties, as well as computer users in general.

Some of our field study findings have been reported elsewhere, including a detailed analysis of a troubleshooting activity [10], a study of system administration tool use and work practices [2], an in-depth analysis of security administrators, their work practices, and environment [8], and a discussion of the limitations of existing administration tools with design guidelines to improve these tools [6]. Our field studies also informed the development of A1/ATMA, a prototype environment to help administrators create and share small tools that automate tasks and perform monitoring [5][9]. Other studies of administration work are few, the most notable exceptions include studies of tasks and tools [1][12], workflow and daily activities [3][7], coordinated activity [11], and collaboration and expertise [4].

2. METHODS
We have conducted 16 field studies in large IT organizations across the US, including corporate data centers, universities, and government laboratories to understand practices of system administrators, operators, team leads, and managers. In these studies we used methods from ethnography, such as naturalistic observation (following sysadmins around with video camera and notebooks as they go through their day-to-day activities in their natural environment), contextual interviews (inquiries in the work place), artifact collection (diaries, instructions, planning documents, etc.), and surveys of larger sysadmin populations.

Our goal was to develop a deep understanding of practice through detailed study of specific cases. Our approach was ethnographic and ethnomethodological, as we studied practices of people in their natural settings and attempted to perform descriptive rather than prescriptive analysis. Field studies have the advantage of providing an exceptionally detailed and accurate portrait of what really goes on in the work place. These observations are often more accurate than self-reports; we've seen several cases where subjects' recollections did not match our video record. Unfortunately, field studies have the disadvantage of relying on a

narrow temporal and population sample. In our studies we were not able to spend more than a week at a time at any given site and the labor-intensiveness of the work limited the number of subjects we could observe. Consequently, we have no doubt that there exist administrators with very different work practices and environments from those we observed, but the commonalities we saw across different sites suggest that our conclusions are valid.

3. SECURITY ADMINS: A BREED APART

Entering the world of security administration one is reminded of spy movies: there are secrets, suspicion, adversaries and collaborators, and work to determine what the other side knows, and whether they know that you know. This environment stems from the secadmin's job: trying to stop malicious human beings from compromising computer systems either directly or through automated agents such as worms, viruses, spy ware, phishing sites, etc. Secadmins go about their tasks through monitoring, analysis, collaboration, and self-education. Interestingly, the human element plays a significant role in both the problem and solution. Below we profile security administration work by analyzing environment and practices in comparison to other system administration specialties.

3.1 Environment: Complexity, Scale, & Risk

In [6] we described dimensions along which system administrators are significantly different from regular computer users. Most notable for this discussion are the dimensions of complexity and scale of computer systems and exposure to risk. Complexity is seen in large computer systems comprised of many heterogeneous components, all of which must work together. Scale is reflected in huge data stores and log files requiring significant time to process. Risk comes from the importance of the systems being managed; failures can lead to unpleasant consequences up to and including job loss.

In the dimension of complexity, security administrators deal with a wider variety of systems and components than other sysadmins. Other types of administrator are usually responsible for specific types of systems or components, deploying new instances, monitoring their operation, and troubleshooting when problems occur. Security administrators, however, must monitor many different types of systems for signs of attack from human or automated agents, stop attacks when they occur, and research vulnerabilities to prevent future attacks. Thus, the responsibilities of security administrators are broad by necessity (though they often don't need to understand the components in as much detail). They need to be aware of all vulnerabilities that could affect any component of any computer system in their organization, and they must work with a variety of other sysadmins to ensure that vulnerabilities are fixed. Repairing vulnerabilities involves an additional level of complexity, however, since the human element involved in attacks gives security problems unusual persistence and dynamism. Computer systems in general do not object to having bugs patched or misconfigurations fixed. Human attackers, however, will often take umbrage at being locked out of a system, and work especially hard to find other vulnerabilities to exploit.

Scale is a huge factor in security work: monitoring an organization for signs of attack often means checking *all* network traffic for suspicious messages or transfers, as well as investigating the behavior of every computer. Given the huge amount of network traffic and numerous computers at an large enterprise or university, secadmins must rely heavily on automated tools to scan and process this data. As an example of the breadth of this monitoring, in [8] we describe a case study where one of the field study researchers, after hearing about a tool used by attackers, did a Google™ search for it and set off automated alarms monitored by one of the security administrators.

Risk is certainly an issue for secadmins, though in different ways from other sysadmins. For example, in our observations we found database administrators very concerned about risk. For them losing data was completely unacceptable, making them extremely meticulous and willing to go to great lengths to mitigate that risk. Database admins would often pair up to double check every command during particularly risky operations. Security administrators appeared to believe that attacks were inevitable, and that some would succeed. We heard the secadmins say that, "any system is compromisable, it's just a matter of time." Exposure of data to outside entities is certainly undesirable, as is destruction of the data by vandals, but meticulousness was not their reaction to these possibilities. For secadmins it was most important to detect and stop attacks as quickly as possible. The secadmins we observed were never separated from their laptops, allowing them to continually monitor their systems. Risk for security administrators is also somewhat more personal. We heard stories of secadmins whose personal computers and websites were targeted in revenge for their professional work, and some of the secadmins we observed made efforts to obscure their job titles and roles from the public. Risk may also be balanced against social responsibility: sometimes secadmins would permit attacks to continue so that they could trace them back to their source and work with law enforcement to prosecute the perpetrators.

3.2 Collaboration and Competition

One approach to manage complexity and risk is through extensive collaboration. Complex systems are made more tractable when expertise is distributed across different people in an organization, yet these people must communicate closely to keep the whole system running. Risk is reduced when multiple sysadmins work on the same problem or process, since many eyes can spot problems and find solutions more quickly. This held true for security administrators as well, we saw them in continual contact with each other sharing knowledge and opinions about suspicious activities, possible vulnerabilities, and ongoing investigations.

Security administration also has a greater learning component than other types of administration work we observed. New vulnerabilities are being discovered daily, so the problem space faced by secadmins is continually changing. They must monitor security and cracking websites on a regular basis to keep abreast of potential security threats. Countermeasures are not always known, so they often download cracking tools and run them in a safe environments to determine how they work and how to act against them. This analysis sometimes reveals vulnerabilities in the attackers' tools, which can be used to track attack activities and trace them back to their source. Security administrators also set up "honey pots", decoy vulnerable systems that are closely monitored to quickly find out when their site is under attack, and how.

As with the world of espionage, computer security is an arena where different groups of people try to gain advantage using

information and secrets. Attackers know about vulnerabilities, and have tools to take advantage of them. Security administrators know about some of the vulnerabilities in their own systems, but also know about vulnerabilities in the attackers' tools. Each side tries to keep its knowledge secret, since when vulnerabilities in the other side's systems become known, they are quickly fixed. Yet security administrators have a community within which information is shared, since an attack on one will probably be replicated on others. Similarly, attackers have a community where they share information on vulnerabilities and brag about their exploits. Information sharing within these communities helps them toward their immediate goals, though it always puts the secrets at risk.

This information warfare is unlike anything we observed in other areas of system administration. In other areas there is an incentive to share information as widely as possible, since there are no antagonists who aim to make systems run less well. With security, however, there is a legitimate desire to keep some aspects of their work confidential.

3.3 Proactive and Reactive

The daily routine for security administrators is much more event-driven than that of other administrators we observed. In general they are responsible for finding problems, but not fixing them. They don't have customers scheduling upgrades or changes to particular systems, instead they are continually monitoring the output of a wide variety of automated security scanning tools. The automated tools are conservative in reporting anything that might possibly be suspicious, so alerts come in frequently and the secadmins must examine each one to determine whether it represents illegitimate activity. In between these interruptions, secadmins engage in research about newly discovered vulnerabilities, and proactive scanning to find vulnerable systems in their organization. They also spend time investigating past attacks and communicating with security professionals at other institutions to understand the breadth of attacks and the wider security environment.

Many types of system administrator use planning, rehearsal, and scripting to mitigate problems of complexity, scale, and risk. When a complex, important operation must be performed in a limited period of time, administrators will often plan in advance and rehearse the operation on one or more test systems, establishing the correct steps to perform the operation and the amount of time required. Scripts or small tools are often created as part of this process to ensure consistent execution. Rehearsal was most common among database and storage administrators, to ensure continued integrity of the data when making significant changes to database or storage organization. We did not see rehearsal used by security administrators, probably because their work didn't involve long, potentially destructive tasks. The primary work of security administrators is monitoring systems, not changing them. Scripting and tool-building, however, was used frequently by security administrators. The secadmins would commonly create small scripts on the fly as part of ad hoc analysis of log files and security scan reports, to help correlate or extract information to help determine whether an automatically generated warning was credible.

3.4 Tools

Security administrators use a wide variety of tools in their work, including automated intrusion detection tools (looking for suspicious patterns in network traffic and computer behavior), scanning tools that check machines for known vulnerabilities, file/host integrity tools which check for viruses and other code used to exploit vulnerabilities, and communication tools such as e-mail, web, chat rooms, etc. As with other types of administrator, the secadmins we observed showed a bias toward command-line tools over GUIs, though there were certainly not averse to using some GUI tools. There is ongoing research into improved visualization tools for security monitoring, though such tools have so far gained limited acceptance (an excellent discussion of GUI vs. command-line security tools can be found in [12], and the issues of GUI vs. command-line for system administration in general are discussed in [6]).

3.5 People and Automation

One of the most remarkable things we observed among security administrators was the amount of human judgment required. Sometimes the only difference between a legitimate and illegitimate action is the person who instigated it. This is a significant departure from other areas of system administration, where the correct operation of a system is much more objective and obvious. For example, in [8] we described an episode where an automatically-generated alert concerning a suspicious file transfer lead to scans of the HTTP log to determine the machines involved and the name of the transferred file, then a search of the machine owner database to determine the owners of the machines, then a Google™ search on the machine-owner's name, and finally a visit to the owner's home page to evaluate whether the file transfer was appropriate given the owner's role in the organization. When passwords can be compromised, an attacker can masquerade as a legitimate user. We heard numerous discussions on automating the process of modeling a legitimate user's normal computer activities so that it would be more obvious when an attacker is logged in to that user's account. For now, it is entirely a judgment call of the part of the security administrators.

4. CONCLUSIONS

Security administrators work practices share many characteristics with other types of system administrator: they are technically inclined people working closely together to manage complex, large scale systems, and there is a fair degree of risk in their work. Working in an environment of ongoing attacks by human antagonists, however, leads significant differences in the types of problems secadmins face. Their work is more event-driven, requires more regular research, and takes place in a tight community with many secrets. Simply put, the human element is the major factor in both the problems and solutions seen by security administrators, and shapes their environment and work practices.

5. ACKNOWLEDGMENTS

Our field study data was the result of hard work by a large team within IBM, including John Bailey, Rob Barrett, Christopher Campbell, Steve Farrell, Cheryl Kieliszewski, Paul Maglio, Madhu Prabaker, Joe Ryan, Leila Takayama, and Anna Zacchi. Special thanks also go to the field study subjects; none of this

work would have been possible without their patience and willingness to perform day-to-day activities while on camera.

6. REFERENCES

[1] Anderson, E. Researching system administration. Ph.D. Thesis. University of California, Berkeley, 2002.

[2] Barrett, R., Kandogan, E., Maglio, P. P., Haber, E. M., Takayama, L. A., Prabaker, M. "Field Studies of Computer System Administrators: Analysis of System Management Tools and Practices." Proc. CSCW 2004.

[3] Dijker, B., A Day in the Life of System Administrators, SAGE, http://sageweb.sage.org

[4] Goodall, John R., Wayne G. Lutters, and Anita Komlodi. (2004) "I Know My Network: Collaboration and Expertise in Intrusion Detection." Proc. CSCW '04, 342-345.

[5] Haber, Eben, Eser Kandogan, Allen Cypher, Paul P. Maglio, and Rob Barrett, "A1: Spreadsheet-based Scripting for Developing Web Tools." Proc. USENIX LISA 2005.

[6] Haber, Eben, and John Bailey, "Design Guidelines for System Administration Tools Developed through Ethnographic Field Studies." Proc. 1st Symposium on Computer Human Interaction for Management of Information Technology, 2007.

[7] Halprin, G. The Workflow of System Administration. In Proceedings of the 6th Annual Conference of the System Administrators Guild of Australia (SAGE-AU '98) (Canberra, Australia, July 6-10, 1998)

[8] Kandogan, Eser, and Eben M. Haber, "Security Administration Tools and Practices." Security and Usability: Designing Secure Systems that People Can Use. Ed. Lorrie Faith Cranor and Simson Garfinkel. Sebastapol: O'Reilly Media, Inc., 2005, pp357-378.

[9] Kandogan, Eser, Eben Haber, Rob Barrett, Allen Cypher, and Paul Maglio, "A1: End-User Programming for Web-based System Administration." Proc. ACM UIST 2005.

[10] Maglio, Paul P., Eser Kandogan, and Eben Haber, "Distributed Cognition Analysis of Attention and Trust in Collaborative Problem Solving." Proc. Cognitive Science 2003.

[11] Sandusky, R. J. Infrastructure Management as Cooperative Work: Implications for Systems Design, In Proceedings of the ACM Conference on Supporting Group Work (GROUP'97) (Phoenix, Arizona, November 16-19, 1997), ACM Press, New York, New York, 1997, 91-100.

[12] Thompson, R. S., Esa M. Rantanen, William Yurcik, and Brian P. Bailey: Command line or pretty lines?: comparing textual and visual interfaces for intrusion detection. CHI 2007: 1205