Security Administration in the Wild:
Ethnographic Studies of Security Administrators

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

INTRODUCTION

System administrators are a crucial population of computer users – they keep our computer infrastructures up and running. Little was known about their work practices and tools, however, spurring us to perform a series ethnographic field studies over the past four years. We made 16 visits across six sites, studying administrators involved in managing system and network security, web hosting, databases, operating systems, storage, and data center operations. Our research methods included naturalist observations of administrators at work (usually recorded on videotape), interviews, surveys, and collection of various artifacts (diaries, manuals, installation instructions, planning documents, etc.).

The details of our findings with respect to system administration have been published elsewhere, including general discussions of work practices and tools [1,2,6], a focus on security administrators [4], and a proposal for a new type of programming environment to help administrators automate tasks and monitoring [3,5].

The goal of this paper is to discuss the advantages and disadvantages of ethnographic studies as a means to better understand security administration. We'll also describe how the lessons from studying the world of the professional, full-time security administrator might be applied to the broader world of security user studies for end-users.

ETHNOGRAPHIC STUDIES

We found ethnographic field studies to be highly effective in better understanding security administration work. Our methods involved two observers spending up to a week at a given site. Our security study involved two such visits in 2004 to a security administration group at a large university. We normally begin with contextual interviews of 30-60 minutes with different members of the group, both to understand the subjects' work in more detail, and also to explain the reasons for our study. After the interviews are completed, we choose one or two subjects to focus on, observing and videotaping the subjects extensively at work. Typically, one of the observers operates the video camera, while the other takes notes and occasionally asks questions to clarify the nature of the subject's actions. We also follow the subjects to meetings whenever possible. Whenever the subject uses an interesting artifact, such as a planning document or list of instructions, we take note and later ask for a copy.

In ethnographic studies it is important to establish the subjects' trust, especially in a sensitive area such as security. The subjects were informed that the videotaping and observation would stop any time they wanted, for any reason (e.g., work in a sensitive area, or a phone call from a girlfriend, etc.) In addition, we let them know that all identifying features in the recordings would be removed before public display. These limitations on recording and display made the subjects more comfortable with being observed. We also found that the subjects were especially motivated when we presented the results from some of our earlier studies – this not only established our credibility as observers sympathetic to the challenges faced by administrators, it also demonstrated how we anonymized our data, obscuring faces and identifying details in video, pictures, and story lines. Any subject could be nervous at the prospect of being filmed, and knowing that their identities are protected helps them to act more naturally in front of the camera.

The results of our studies are a highly detailed record of how an administrator works, minute-by-minute, throughout the day. The written notes capture the larger context, and serve as an index to activities, while the video records details of what they read and write on their computer, who they call on the phone or talk to in person, and their emotional state in different situations. We can follow problems from discovery to resolution, see which tools were used and how frequently, and even determine the details of collaboration between people. We capture the full richness of daily activity, recording how subjects spend their time, where they face problems, and how they resolve them. In fact, we've found our data was sometimes more accurate than the subject's own reporting – when asking subjects about events we taped, we found that they didn't always accurately recall which problems took up their time. People often don't realize where their time goes.

While ethnographic data is invaluable, gathering and analyzing the data is extremely labor-intensive, resulting in a relatively small population and temporal sample (more than once we were told, "you should have been here last week…"). It is theoretically possible to use the null hypothesis to make statistical claims based on field study results (e.g., nine of ten subjects were observed to experience problem X, therefore the probability that X is *not* a problem for at least 50% of the general population is…), yet it is usually quite difficult to assess how representative the subjects are as a population. The intrusive nature of observation and videotape can also be an issue, especially with sensitive work such as security administration. We have been unsuccessful in several instances gaining permission to observe and/or videotape in certain commercial and government settings, and there is always the question of whether subjects behave normally when being observed. Our experience suggests that they get used to being observed within a few hours, but this is difficult to prove. It is impossible to be truly unobtrusive when observing a subject in their own work setting, but we aimed to reduce our impact as much as we could. In addition, the real world is not predictable, and what happens during your observation may not answer the specific questions you started with. For example, the computer systems might not be under attack during your observations, limiting what you can learn about security crises. On the other hand, we believe studying subjects and their work in context offers invaluable information particularly when work is idiosyncratic, event-driven, and informal as in security administration.

In balance, we have found ethnographic field studies to be very useful in understanding the tools and work practices of security administration, and despite the disadvantages the results are compelling. It is the best way to capture the full complexity of real-world situations and interactions, and videotape really helps audiences understand and sympathize with the study subjects.

SECURITY ADMINISTRATORS

The results of our security administration studies are described in detail in [4], but we will describe some of the important conclusions, particularly as they relate to conducting further ethnographic studies.

We studied a group of professional security administrators at a large university. The task of securing several hundred computers involved many aspects: continual research to learn about new exploits, running scans for different vulnerabilities, interpreting the output from automated monitoring and scanning tools, reacting to intrusions (either by shutting them down immediately, or allowing them to continue to trace them back to the source), establishing and updating security policies, and even setting up "honeypots", dummy machines to lure attackers and gain information about them.

Security administrators use a wide variety of tools to perform these tasks, from web browsers, IM, and e-mail, to specialized tools for analyzing large volumes of data (network traffic, file systems). Administrators often create their own tools, to manage the specifics of their own systems and circumstances. Work is often informal and consequently great deal of human judgment is required, since the automated monitoring tools err on the side reporting everything that might be suspicious. For example, we witnessed one episode where the automated tool reported a file transfer from a formerly-compromised machine, and the administrator needed to examine the file and research the machine's owner to ensure that it was legitimate.

We found security administration work practices vary by the particular instances of security incidents. Although administrators try to specialize, every new incident is different and requires new knowledge and research. Administrators thus heavily rely on the community and we found security administrator community particularly closely knit. Collaboration was extremely important, as different administrators shared information and questions about ongoing events affecting their systems.

Security administrators are at an extreme when compared to "average" computer users. Security is their primary task, and they deal with more machines, more network traffic, and more attacks than anybody else. Naturally, the work of the security administration is very event-driven, as incidents come and go. Keeping an end-user's computer secure requires many of the same activities as are performed by a professional administrator: scanning, monitoring, learning about new vulnerabilities, but these activities must be automated/outsourced for the end-user (who doesn't want to think about security every minute of the day). The result for end-users are tools such as automated, self-updating virus scanners, firewalls, and phishing detectors. User testing such tools is difficult, given the low profile that security has for end-users, and the infrequency of attacks. We have described how a large university setting is ideal for conducting ethnographic studies of security administrators, yet one could also use these administrators as a gateway for studying end-users. In a large university setting, the size and heterogeneity of the computer and user populations and public nature of the institution ensure that attacks/viruses/worms will be more likely than other settings. While security-events happen seldom to any individual, a wide deployment across many users could be monitored from the security administration offices - when an end-user is under attack, the security administrators are usually the first to know.

CONCLUSIONS

In conclusion, ethnographic field studies offer invaluable insight when studying security. Ethnography is powerful approach for generating an extremely detailed portrait of a user's work practices and tools. When a user's primary focus is security, as in the case of security administrators, field studies can greatly help understanding the usability of security tools and techniques. Ethnography is less useful when security-related events are rare, though in such cases security administrators could serve as a gateway to finding and monitoring end-users working with security tools.

REFERENCES

[1] Bailey, J., Etgen, M. & Freeman, K. Situation awareness and system administration. In Barrett, R., Chen, M., & Maglio, P. P. (Eds). *System Administrators are Users, Too: Designing Workspaces for Managing Internet-scale Systems*, CHI 2003 Workshop.

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

[4] 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. http://www.plunk.org/eben/PublishedPapers/Security-ch18.pdf.

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

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