HOT Admin: Human, Organization, and Technology Centred Improvement of IT Security Administration

David Botta, Rodrigo Werlinger, André Gagné
Konstantin Beznosov*, Lee Iverson, Brian Fisher, Sidney Fels

University of British Columbia, Vancouver, Canada

September 12, 2006

Introduction

Cryptography, access control, network security, and other security technologies have been actively studied and developed in the past some forty years; thousands of papers devoted to the individual technological topics have been produced. Yet, if the person administering these technologies can't work with them, what use are they? Organizations rely on their security infrastructure in order to operate in the day to day, most of the time adding more and more security devices each time a security breach arises. Nevertheless, vulnerabilities in information technology (IT) services are far from disappearing.

Our project towards **H**uman, **O**rganization, and **T**echnology centred improvement of information technology (IT) security **admin**istration (HOT Admin) addresses the security issue from a holistic perspective, focusing on the integration of human and organization aspects with the technological ones. To our knowledge this is the first attempt to address systematically the interaction of security administrative models and technologies with usability within an organization.

Goals

To improve IT security administration (SA), this project aims to achieve two overarching goals: first, to devise a methodology for evaluating the effectiveness of IT security administrative tools; second, to design effective technological solutions, guidelines, and techniques to aid security administrators.

Approach

Our approach considers the problem as the interaction of three main factors: human, organizational, and technological (HOT). Given this context, we will conduct field studies of security administrators in real, complex organizations in order to characterize their roles, responsibilities, interactions with others, the tasks they perform, and the tools they use. Analysis of this data will then allow us to bring together the human, organizational, and technology centred approaches to form guidelines and techniques for the creation of advanced security administration systems and their evaluation.

*Contact author. beznosov@ece.ubc.ca

Current Work

The project is in its first phase. The field study involving industry organizations is about to start. The overall goal of this field study is to study security administrators in order to understand and model their tasks as well as the effectiveness and usability of the tools they currently use to perform these tasks. Specific objectives are: 1) provide inventories of a) security administration errors, b) how constraints and limitations manifest in the human, organizational and technological dimensions, and c) technologies; 2) provide rich data about the security administration task space. We expect that the study will use the living context of the security administrator's activities, and therefore will require a *case study* approach. We will tune the case study design with a pilot study.

The rationale for the study design was taken from research questions that were generated by the project team through discussions. The questions target as many aspects of the human, organizational, and technological dimensions that both were feasible and contribute to the research goal.

The instrument comprises a pre-interview questionnaire, a semi-structured interview, and a contextual interview. A factor that influenced the nature of the instrument was the granularity of data that we felt appropriate to research questions such as: *"How are tools and their parts used?"* To illustrate, an interviewer can ask the subject to elaborate in detail about tool use with respect to situations in the past, while observation of the subject at work could reveal how the subject recovers from interruptions.

We will be recruiting subjects from organizations ranging from as small as local offices of five employees to as large as world-wide with several thousand employees. They will be in a variety of industries from production to accounting to IT Security. We will solicit participation of the subjects by contacting them over e-mail.

Using the information gathered from the field study, we will develop guidelines and techniques for designing more effective technological solutions for IT security administration. To validate our guidelines and techniques, we will use them to build sample tools for specific areas of IT security administration and test them in the concluding field study, which will involve our industry partners and other organizations.

We will present the project, design of the field study of security administrators, and the preliminary results of the

study. We expect to have conducted several interviews by the end of November 2006.