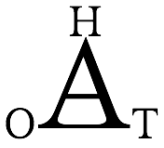

HOT Admin:
Human, Organization, and Technology Centred Improvement of IT Security Administration

Objectives

1. To devise a **methodology for evaluating the effectiveness of IT security administration tools**;
2. To develop **guidelines and techniques for designing effective tools** for security administrators.

Problem

The management of IT security is an enormous, difficult, and costly problem. Yet little is known about security administrators, the nature of their work, and how effective their tools are. Much like an air-traffic controller, if a security administrator makes an error, entire organizations may be compromised leading to, in the best case, loss of productivity and, in the worst case, injury or death to people.

Approach & Deliverables

We will advance the understanding of IT security administration as a distinct human activity to the level at which comprehensive **human**, **organizational**, and **technological** models of IT security administration can be used to achieve the project objectives.

We will involve our industry partners or their customers in the field studies to

1. analyze the **task space of security administrators**,
2. create an **inventory of the common types of errors** made by security administrators,
3. develop an **inventory of the conflicts of forces** that cause errors in security administration,
4. create an **inventory of the technologies** employed for security administration, and
5. analyze **organizational structures** that prevail nowadays.

These five initial results will allow us to develop a **mental model of security administrators**, an **organizational model**, and a **model of the underlying technologies** used for security administration. These three models will make it possible to realize the practical deliverables of the project. As the result of creating the above models, we will be then in a position to develop a **methodology for evaluating tools and technologies** for security administration, as well as **guidelines and techniques for designing such tools**.

The methodology will be intended for evaluating security administration tools and user interfaces, and their effectiveness not only in terms of usability but also in terms of their ability to support the understanding (mental models) of security-related system state, administrative actions, and their repercussions in terms of security and workflow within the organization. We will develop guidelines and techniques for systematic design of security administration tools and UIs.

Finally, to test the feasibility, validity, and the claimed benefits of our findings, we will develop **sample tools for security administration** using our design guidelines and techniques, and compare their effectiveness with the state of the practice in the exit field study.

Expected Results & Benefits

Our industry partners will get several immediate and very practical benefits. We will provide the companies who participated in the studies with the results that are expected to identify

- **common types of errors** made by their security administrators,
- inventory of the **conflicts of forces** that cause errors in security administration,
- inventory of the **technologies** employed for security administration,
- analysis of the **organizational environment** that encapsulates the administrators' workspace.

Plan

1. **Pilot studies**: We will start with small-scale short pilot studies with the University of British Columbia (UBC) IT services. The pilots will allow us to establish and validate our study methodologies for the larger-scale follow ups (items 2 and 7),
2. **Initial field studies**: we will involve our industry partners to perform field research to develop the foundation layer of the project. We believe that there are task-specific conflicts of forces that drive administrators into making errors. This field studies will be an opportunity for us to investigate these conflicts. Collected data will be used as a reference point for the development of our theoretical approach to modeling the security administration processes and the administrators themselves. User organizations participating in the studies will directly benefit from them by having access to the specific outcomes, including organization-specific causes of administrative errors.
3. **Models**: Based on the results of the initial field studies, we will develop a mental, organizational, and technology models of security administration as a distinct professional activity.
4. **Evaluation methodologies**: We will use the above models to develop a methodology for evaluating the effectiveness of the technological solutions employed for IT security administration.
5. **Design guidelines and techniques**: We will develop guidelines and techniques for designing effective technological solutions for IT security administration.
6. **Sample tools**: To validate our guidelines and techniques, we will use them to develop sample tools for specific areas of IT security administration and test them in the concluding field study.
7. **Concluding field studies**: To test the sample tools and to verify the effectiveness of our approach, we will run a second set of field studies involving our industry partners and other organizations.

Team

Prof. Konstantin Beznosov has five years of industrial experience when he worked on enterprise security architectures for health care, telecom, and financial organizations. He founded the Laboratory for Education and Research in Secure Systems Engineering. Beznosov's primary research expertise is the **engineering of secure systems** with particular focus on **designing security mechanisms** for distributed information systems, **engineering secure software**, and **access control models and architectures**. He leads the technology thread of the project and administers the project.

Prof. Sidney Fels has extensive expertise in **HCI** and **interface design**. He is the founder and director of the Human Communication Technologies Laboratory. Fels works on usability studies and testing procedures, and guides the design and development of prototypes as well as data analysis for the project.

Prof. Brian Fisher is an Associate Professor of Interactive Arts and Technology at Simon Fraiser University and an Adjunct Professor in Management Information Systems and Computer Science at UBC. His area of expertise is in **cognitive science-based interaction design**. Fisher is involved in testing methodologies and design guidelines in the HCI thread of the project.

Prof. Lee Iverson has an extensive background in **information visualization** and **information systems**. His work is focused on **collaboration infrastructure** and **security usability**. Iverson is leading the project in the investigation of the organizational forces pertinent to security administration.

Support

The project is financially supported by Natural Sciences and Engineering Research Council (NSERC) of Canada (CAD $459,000 for three years). The following companies have expressed in written the support for the corresponding grant proposal submitted to NSERC: Entrust, SAP Labs Canada, Recombo.

Further Info. & Contacts: https://lersse.ece.ubc.ca/tiki-index.php?page=Project_HOT-Admin