Identifying Difference between Security and other IT Professionals: a Qualitative Analysis

André Gagné, Kasia Muldner,

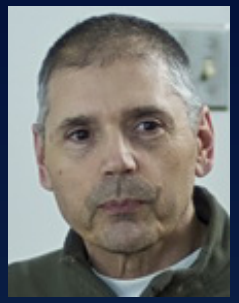
Konstantin Beznosov

Department of Electrical and Computer Engineering

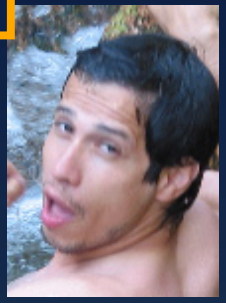
University of British Columbia

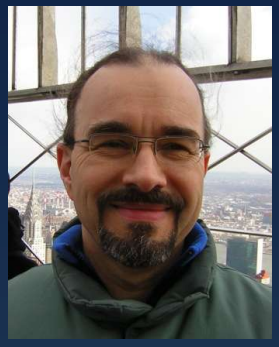
Project Team

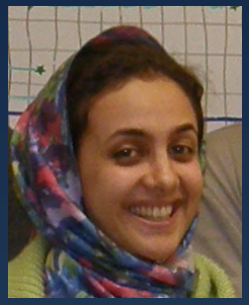
Dr. Konstantin Beznosov
- Principal investigator (PI)
- Assist. Prof., ECE, UBC
- security; 5 years of industry

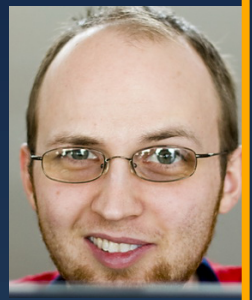


Dr. Sidney Fels
- Assoc. Prof., ECE, UBC
- new interfaces design









Dr. Brian Fisher
- Assoc. Prof. of Inter. Arts and Techn., SFU
- Adjunct Prof. in MIS and CS, UBC
- cognitive science-based interaction design

Dr. Lee Iverson
- Assist. Prof., ECE, UBC
- Inform. visualiz.
- collaboration infrastructures

Outline

- Research context
- Related work
- Methodology
- Results
- Conclusions & future work

Research Context

Security professionals (SP) vs. other IT professionals

Related Work

- Some work does not distinguish between security and other IT
  - IT professionals need better tool support [Haber&Bailey 2007]
  - IT work requires variety of skills, e.g., collaboration [Barret et al. 2004]
  - IT tasks: end-user training, maintenance, reconfiguration [Anderson 2002]

Related Work

- Other research focuses on security professionals (SPs):
  - SP face many challenges, e.g., distribution, lack of management buy [Siegel 2006]
  - Security vs. other IT: SPs deal with higher complexity [Haber&Kandogan 2007]

Research Context

- Research question:
  - What differentiates security from IT professionals?

Motivation:

- Understanding of differences needed to design support tailored to security professionals' (SP) needs

Methodology

in situ semi-structured interviews

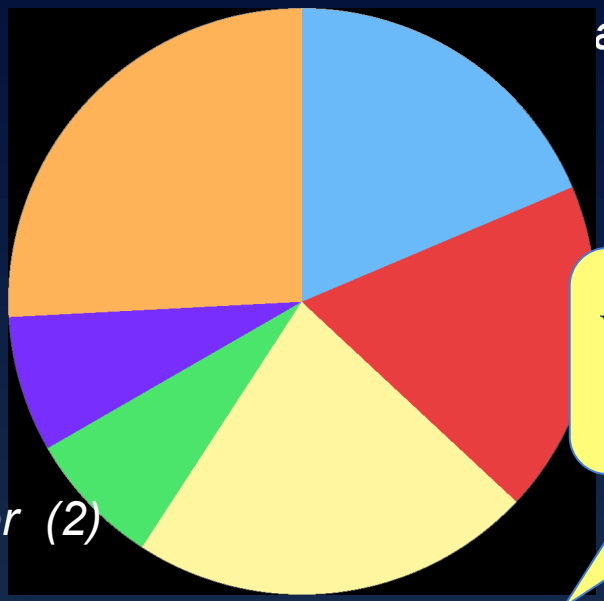
- 1 - 1.5 hours in duration
- Variety of questions:
  - What differentiates security from general IT?
  - What kinds of challenges do you face?
  - What tools do you use? What do you like / dislike about your tools?

Participants = 27 Profes

Manages all aspects of IT

Works in a specific IT area

Performs a diverse range of security-related duties



anager (5)

(6)

including staff, policy design, etc.

l (2)

Security: Manager (2)

Works in a specific security area

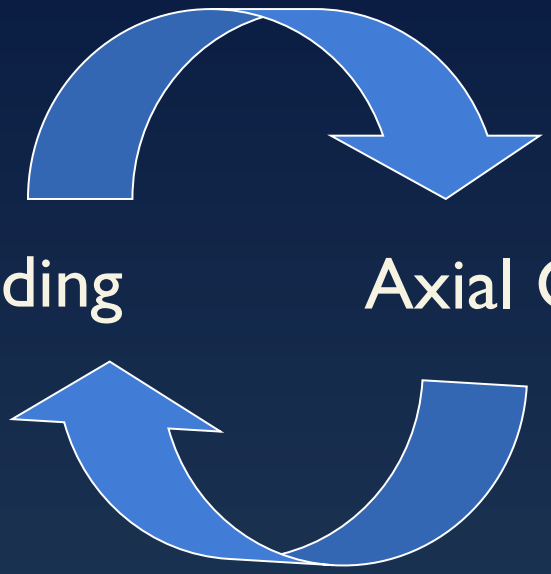
diverse range of IT-related duties, including security

Security: Specialist (7

- Across a variety of different organizations
  - Education, manufacturing, financial services, consulting, insurance, research, non-profit, retail, scientific services

Data Analysis

- Transcription + sanitization
- Qualitative description



Open Coding

selection of categories that arise from the data analysis

Axial Coding

synthesis and refinement of the data, to make explicit the connections between the categories

Coding Example

Do you think that there's a difference between security-related tasks and other IT tasks? Can yo[u] [m]ake security different?

Security hinders users

Well a very glib answer would be that they are different because security involves making things more difficult for people rather than not. Like I said, that's a glib answer and not necessary completely true but the element of truth in that is [t]hat if there is a security problem, the solution is to get people to stop doing [w]hatever it might be. If someone wants to run a file-sharing program on their [c]omputer don't do this because it opens us up to X Y and Z. That leaves them frustrated. Or, don't go to that website, well but they want it, and like I said those are very glib answers and only cover certain cases where you are telling people don't do the thing that involves exposing us to problems.

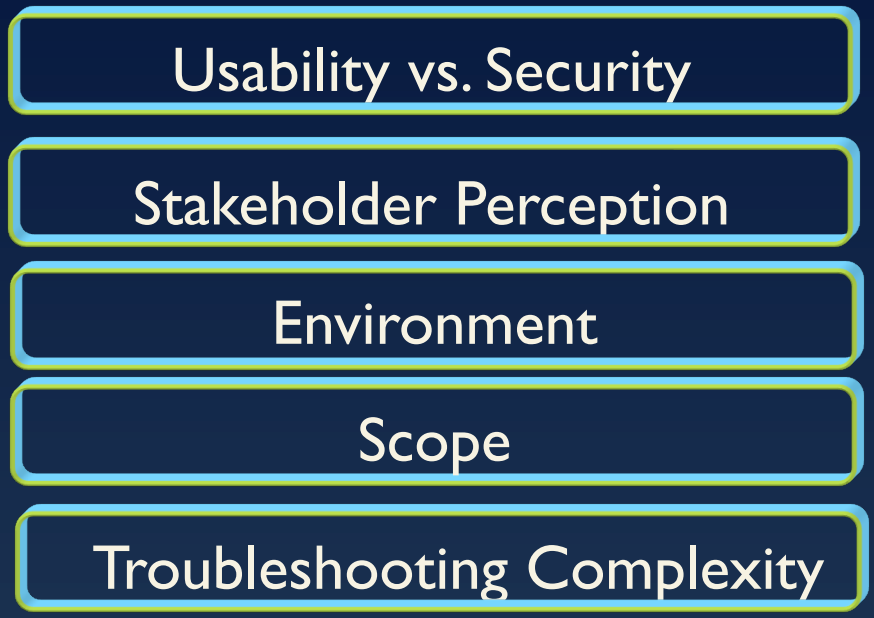
Security vs. Usability

A lot of the time the other IT stuff, the non-security related IT stuff tends to be helping people get their work done in more or less immediately visible way. I can't get my e-mail or, here's how. I can't [s]end e-mail this way sucks. Well let me take three months and get a good web mail program. The server went down for the third time today, okay; let me spend three months getting a better server and redundant servers and things like this.

IT helps users

Results

- Identified differences between security and other IT along the following dimensions:



Usability vs. Security

Security professionals need to balance usability and security

> *"I think it [security and general IT] is different because you have to balance the usability of the system [with its] security."*

Increased security is often a hindrance for people, but…

increased usability may decrease security

Stakeholder Perception

Security professionals (SPs) are perceived in a less positive light by organizational stakeholders

SPs have to raise security awareness via education, innovative campaigns, etc.

Environment

IT technological landscape: rate of change

"IT is a fast changing field and security is even faster"

Threats: only SPs have to contend with active and continuous threats

Security practitioners need a fast response time, must stay up to date

Maintaining Scope

SPs need broader internal scope than other IT professionals

> *"you really need to be able to look quite wide and deep.*

SPs need broader external scope

- Legislation (Patriot Act, Sarbanes Oxley)

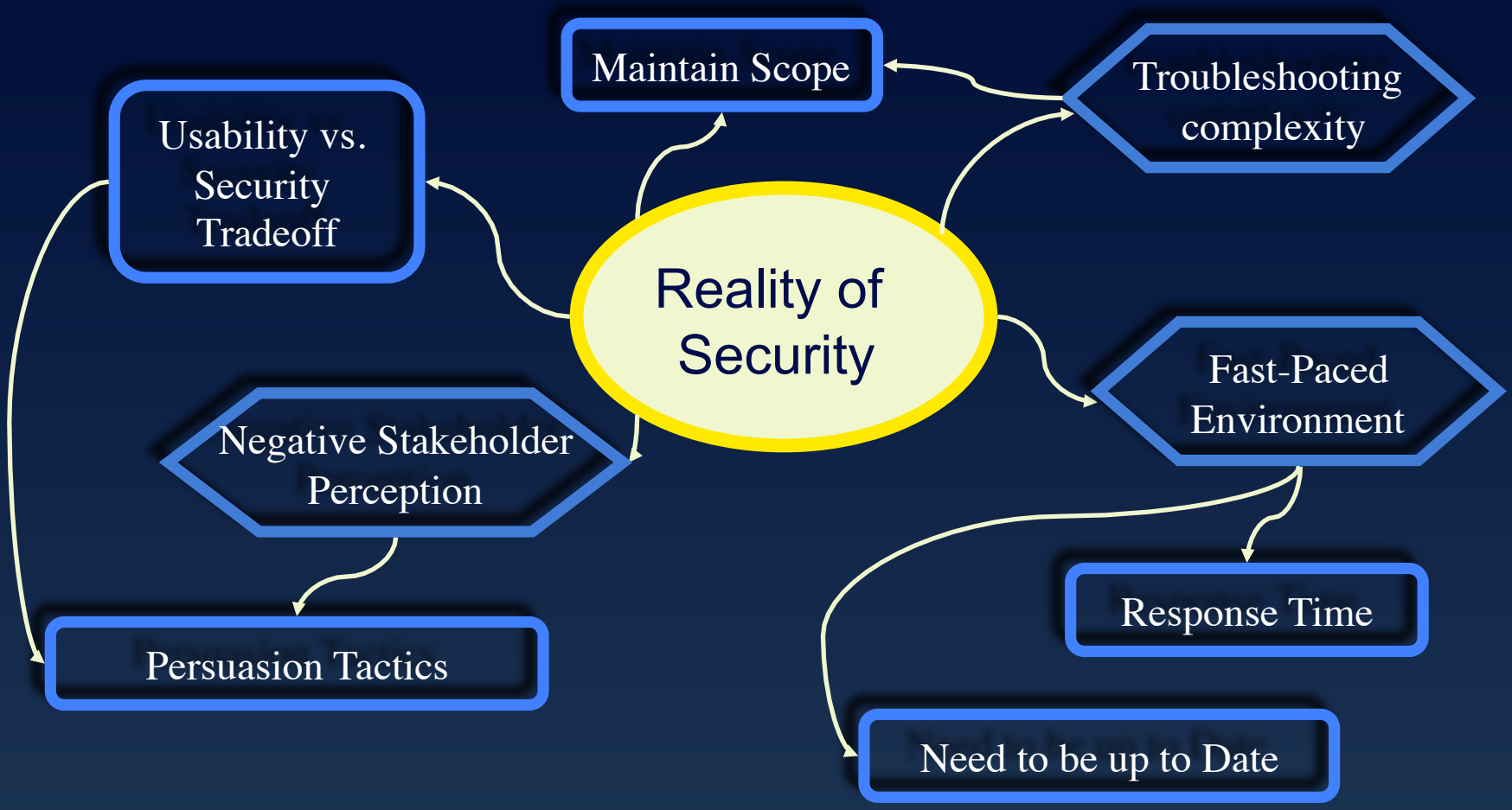
Troubleshooting Complexity

Security tasks entail a higher level of complexity:

- Have to "*go through more steps*"
- Need to collaborate with other stakeholders
- Sensitive nature of the process

> *"you cannot jump to conclusions and assume someone is guilty ... more is at stake than simply how fast the system is recovered"*

Model Relating Differences



SP's behaviors

Factors that influence SPs'

Lowering the Burden

- Troubleshooting Complexity
  - Scaffolding via tools for distributed nature of IT security
  - Reification of tacit knowledge
- Influence Stakeholder Perception
  - Via management buy in [Siegel et al. 2006]
- Mitigate need for usability/security tradeoff
  - Shift in design culture [Smetter & Grinter 2002]
  - Stakeholder involvement during design process [Flechais & Sasse in press]

Conclusions

- Identified differences between security and other IT professionals
- Validated and extended related work
  - Increased sample size (more participants and organizational sectors)
  - Exposed differences related to organizational factors
  - Provided model of differences
- Differences increase complexity -> we provide suggestions for related support

Future Directions

- Refine the model with additional data and analysis
  - How are differences between security and other IT influenced by
    - organization type
    - organizational sector
    - participant position
- Identify solutions that we borrow from general IT to support security practitioners

Thank-you for your attention!

Web: www.hotadmin.org

Email: kmuldner@ece.ubc.ca