Human, Organizational and Technological Factors of IT Security

Kasia Muldner

The HOTAdmin Project

LERRSE Lab, Department of Electrical and Computer Engineering

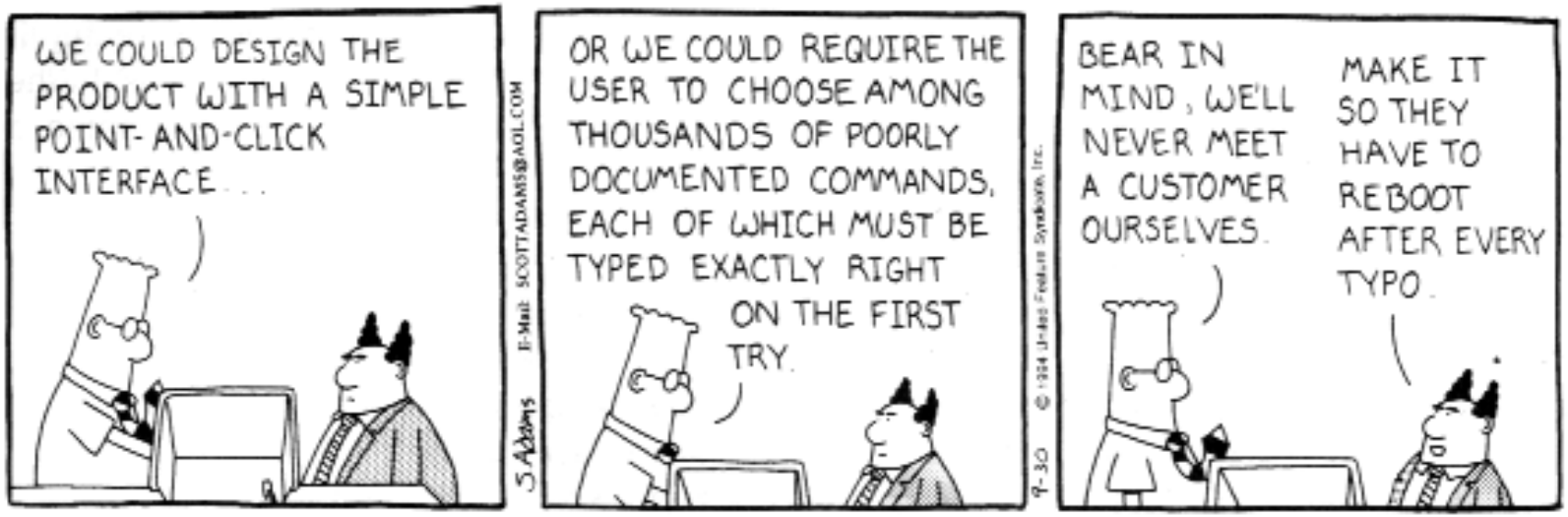
University of British Columbia

When is a System "Secure"?

"A computer is secure if you can depend on it and its software to behave as you expect."

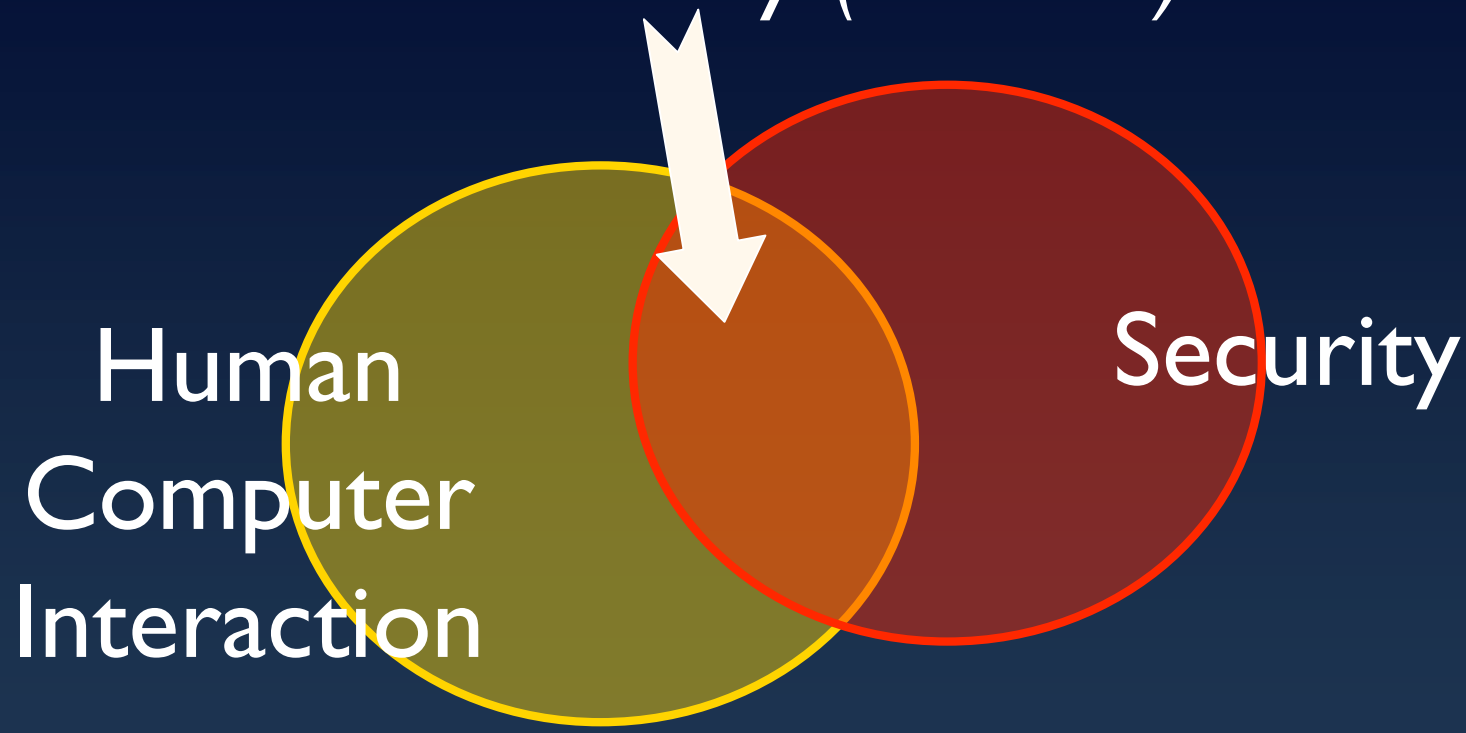
Garfinkel and Spafford, "Practical Internet Security"

Who is the Weakest Link?



DILBERT reprinted by permission of United Feature Syndicate, Inc.

Usable Security (HCISec)



Usable Security Challenges

- Security is a secondary task ➡ how to motivate users?
- Wide range of users ➡ how do to support different types of users?
- Negative impact of errors ➡ how to minimize the damage?

Usable Security for All Users

- HCISec is a growing field
- To date, focus has been on ways to support the single end-user
  - Password managers (e.g. Chiasson, Biddle et. al)
  - Prevention of phishing attacks (e.g. Wu, Miller et. al)
- What about IT professionals that are responsible for upholding security in their organizations?

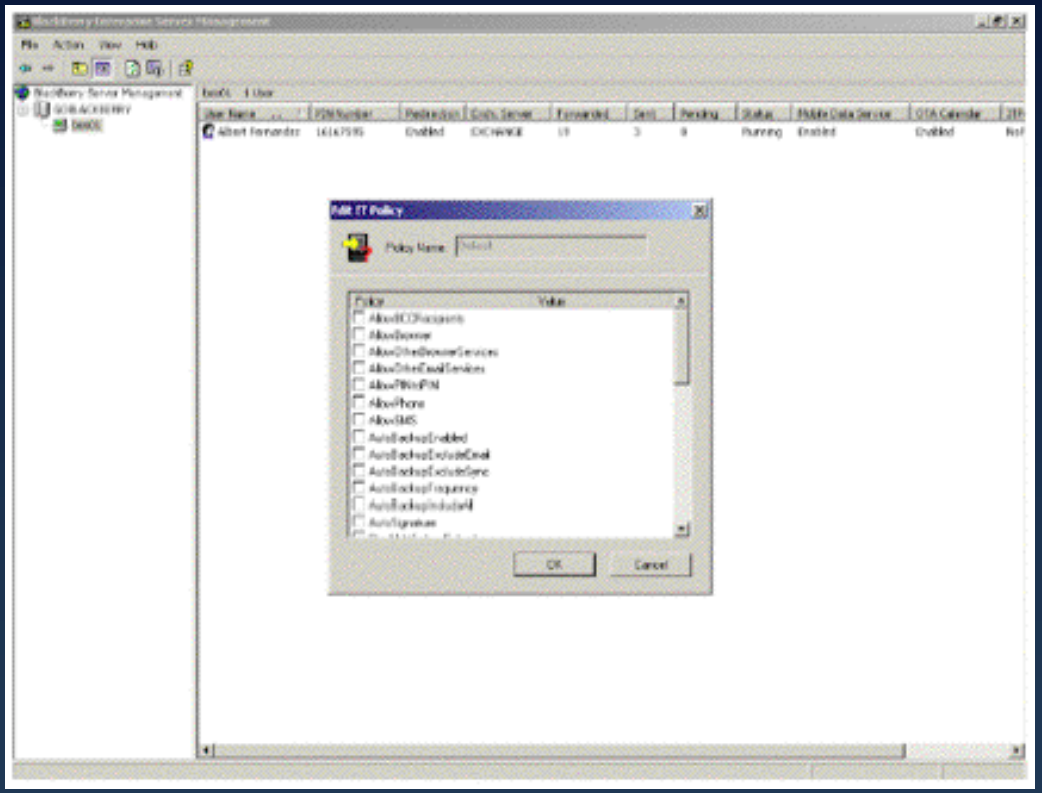
Hypothetical Example

ABC Inc.
large company
with 5 divisions

Jenny Smith
ABC's senior security administrator

Business policy: All e-mail messages between senior management must be end-to-end secure

Blackberry Enterprise Server Management



Configuring BES to Enforce the Policy

First:

1. Turn MIME (S/MIME) encryption on
2. Enable S/MIME encryption for the user

Set alpha-numeric rules:

3. Cert. Status Cache Timeout
4. Cert. Status Maximum Expiry Time
5. FIPS Level
6. S/MIME Allowed Content Ciphers
7. Trusted Certificate Thumbprints

Set to False

8. Allow Other Email Services

Set to True:

9. Disable Email Normal Send
10. Attachment Viewing
11. S/MIME Force Digital Signature
12. S/MIME Force Encrypted Email
13. Disable Invalid Certificate Use
14. Disable Revoked Certificate Use
15. Disable Stale Status Use
16. Disable Untrusted Certificate Use
17. Disable Unverified Certificate Use
18. Disable Unverified CRLs
19. Disable Weak Certificate Use

Total 19 steps!

That's Not All!

- Now do (most of) the same for other senior managers
- Now do the same on the other four servers

Is this security technology "usable"?

Limitations of the GUI

- Which of the 140 rules need to be set?
- How to remember which values to set the rules to?
- Difficult to determine the results of changes?

Motivation

- Protecting organizations is becoming increasingly challenging for security professionals:
  - The perimeter is dissolving
  - IT attacks are becoming more pervasive and advanced
- Usable security solutions are lagging behind the bad guys

Outline

- HOTAdmin project: introduction
- Field study
- Results
- Conclusions & future work

HOTAdmin

- HOT: Human, Organizational and Technological
- Goal: advance the state of usable security solutions for security professionals
- Challenge: little real-word data exists on security professionals: how they work & what tools they need

HotAdmin Team

HOTAdmin Overview

Field Study

Analysis & Model Development

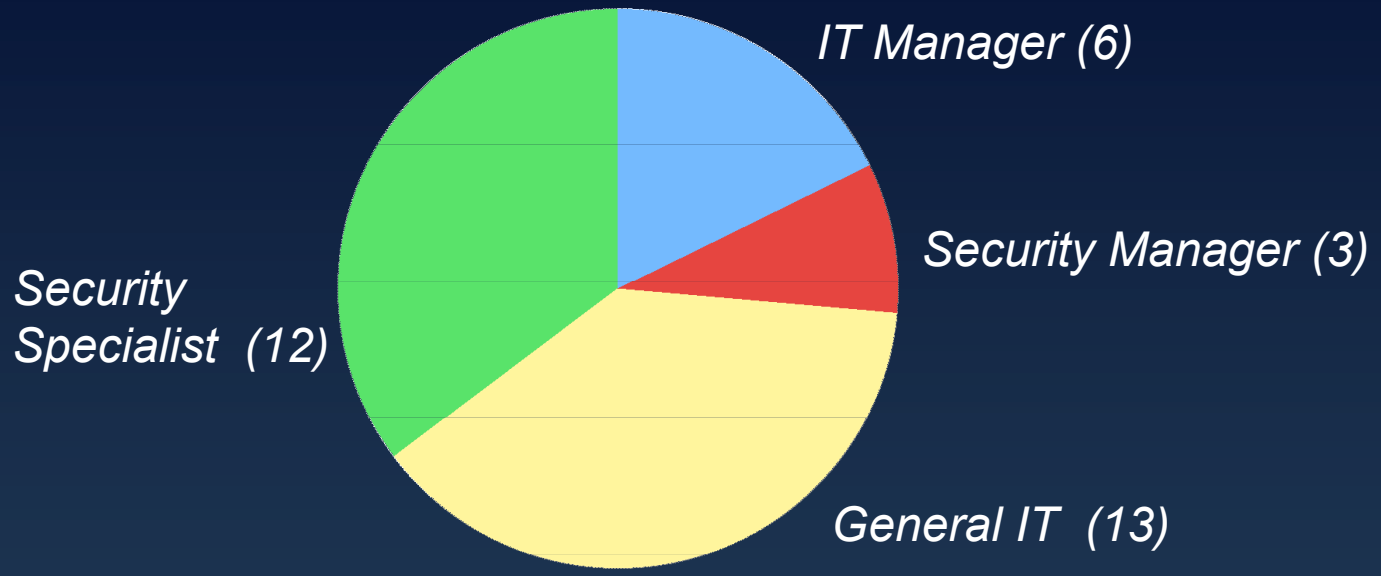
Guidelines for Tool Design

Validation of the Results

"Towards Understanding IT Security Professionals and Their Tools", SOUPS'07.

Field Study Participants

- 34 Professionals



- Across 16 different organizations
  - Academic, manufacturing, financial services, consulting, technology, insurance, scientific services, government, non-profit, retail, telecommunications

Field Study Methodology

in situ semi-structured interviews

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

HOTAdmin Overview

Field Study

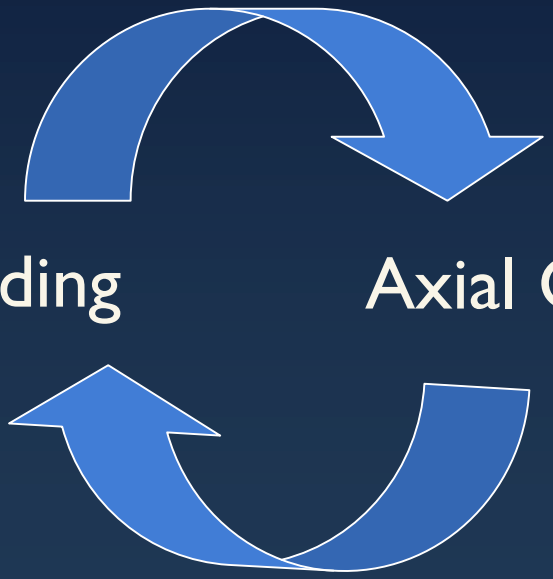
Analysis & Model Development

Guidelines for Tool Design

Validation of the Results

Data Analysis

- Transcription + sanitization
- Qualitative description [Sandolowski]



Open Coding

Axial Coding

selection of categories that arise from the data analysis

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 … asks? Can you talk about what makes security different?

Security hinders users

Well a very glib answer would be that they are differ… because security involves mak…g things more difficult for people rather than not. Like I said, that's a glib a…wer and not necessary completely true but the element of truth in that is that typically if there is a security problem, the solution is to get people to stop doing that - whatever it might be. If someone wants to run a file-sharing program on the computer - ve…

Security vs. Usability

because it opens us up to X Y and Z. That leaves them bored and frustrated. Or, don't g… they want it, and like I said those are very glib answers and only cover certain cases wh…re don't do the thing that involves exposing us to problems.

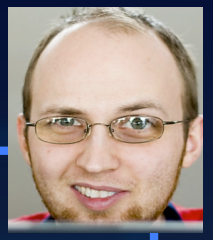
A lot of the time the other IT stuff, the non-security related IT stuff tends to be helping people get their work done in a more or less immediately visible way. I can't get my e-mail or, her…s how. I can't print, here's how. Checking mail this way sucks. Well let … take three months and get a good web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

IT helps users

More generally I would say they are different because - partly because security problems can involve potential privacy issues, so you are scanning mail for spam or for viruses - yes it's done by a computer but at some point you will probably have to go check it about a porn (?) case. And that will involve saying can I look at your e-mail, can I look at your files. I am always conscious of asking permission to do that sort of thing, and giving people the option to say no. …

Results

- Field Study
- Analysis & Model Development
  - Security vs. IT
  - Challenges
  - Interactions
  - Errors
  - Tasks & Tools
  - Management Model
- Guidelines for the Design of Techniques
- Validation of the Results

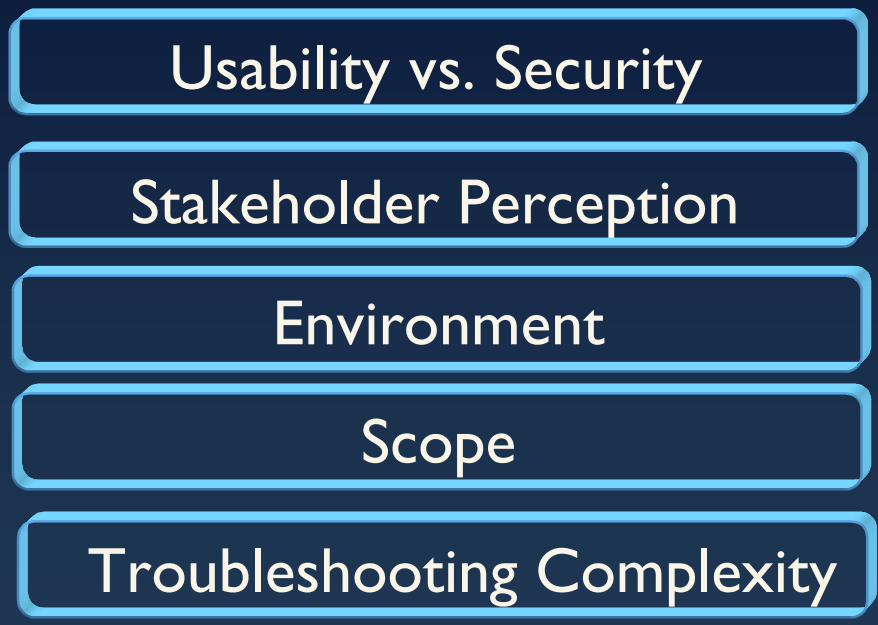


Theme: Security vs. IT

- Research question:
  - *What differentiates security and general IT professionals?*
- Motivation:
  - To date, related work has focused on studying system administrators without isolating security aspects
  - This makes it difficult to design support tailored to security professionals' (SP) needs

Results

- Differences between security and IT along the following dimensions:



"Identifying security professionals' needs: a qualitative analysis", submitted to HAISA'08.

Results (con't)

Usability vs. Security

Security professionals are constantly balancing 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. You can have a foolproof security system but it's not going to be very usable… the most secure system is when it's turned off, and behind locked doors"*

Results (con't)

Stakeholder Perception

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

Environment

Changing technological landscape

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

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

Results (con't)

Scope

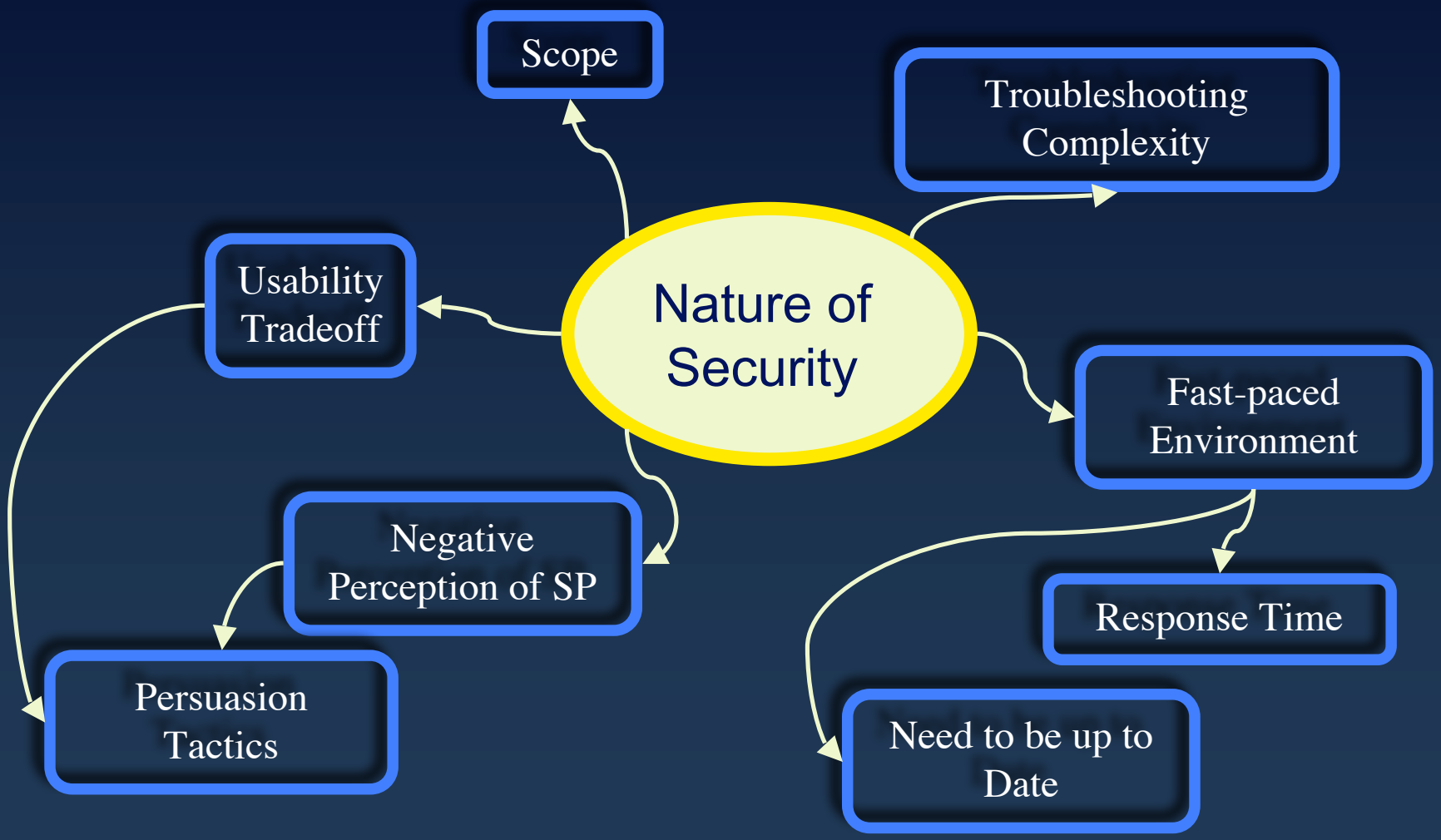
SPs need broader internal scope than general IT

"you really need to be able to look quite wide and deep. You need to be able to look within the packet in a lot of detail to understand how an intrusion detection system works… And at the same time you need to take a wide look to an organization to be able to determine … the risks…. And that differs from IT where other groups can really be focused in one particular area"

SPs need broader external scope than general IT

Legislation (Patriot Act, Sarbanes Oxley)

Model of Differences

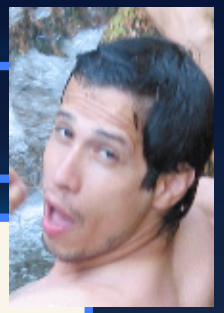


Summary

- Differences between security and general IT professionals increase the overall complexity SPs have to contend with
- Implications?
  - Reduce the burden, e.g.:
    - Via innovative usable solutions to mitigate need to balance security
    - Via tools that integrate organizational information to facilitate wide overview (scope)

Results

- Field Study
- Analysis & Model Development
  - SP vs.. IT
  - Challenges
  - Interactions
  - Errors
  - Tasks & Tools
  - Management Model
- Guidelines for the Design of Techniques
- Validation of the Results



Theme: Challenges

- Research question:
  - *What are the key challenges SPs face and how do they interplay?*
- Motivation:
  - Related work has studied challenges *in isolation*
  - This fails to provide a holistic account of the human, organizational and technological forces

Results

- Challenges classified among the following dimensions:

Human

Organizational

Technological

"Human, Organizational and Technological Challenges of Implementing IT Security in Organizations", submitted to HAISA'08.

Challenges: Human

Culture

Poor security practices → difficult to implement security controls

Training

Security practitioners lack the necessary training

Communication

Lack of common view among stakeholders → difficult for SP's to communicate *risks* and security issues

Challenges: Organizational

Risk Assessment	Difficult to estimate IT security risks
Business Relationships	Misaligned security policies make it challenging to enforce standards within an organization
Security Low Priority	Security is not a priority for many stakeholders
Task Distribution	Distribution of responsibilities was an issue: "*the decentralized nature does not help*"…
Open Environment	
Tight Schedules	
Data Access	
Budget	

Challenges: Technological

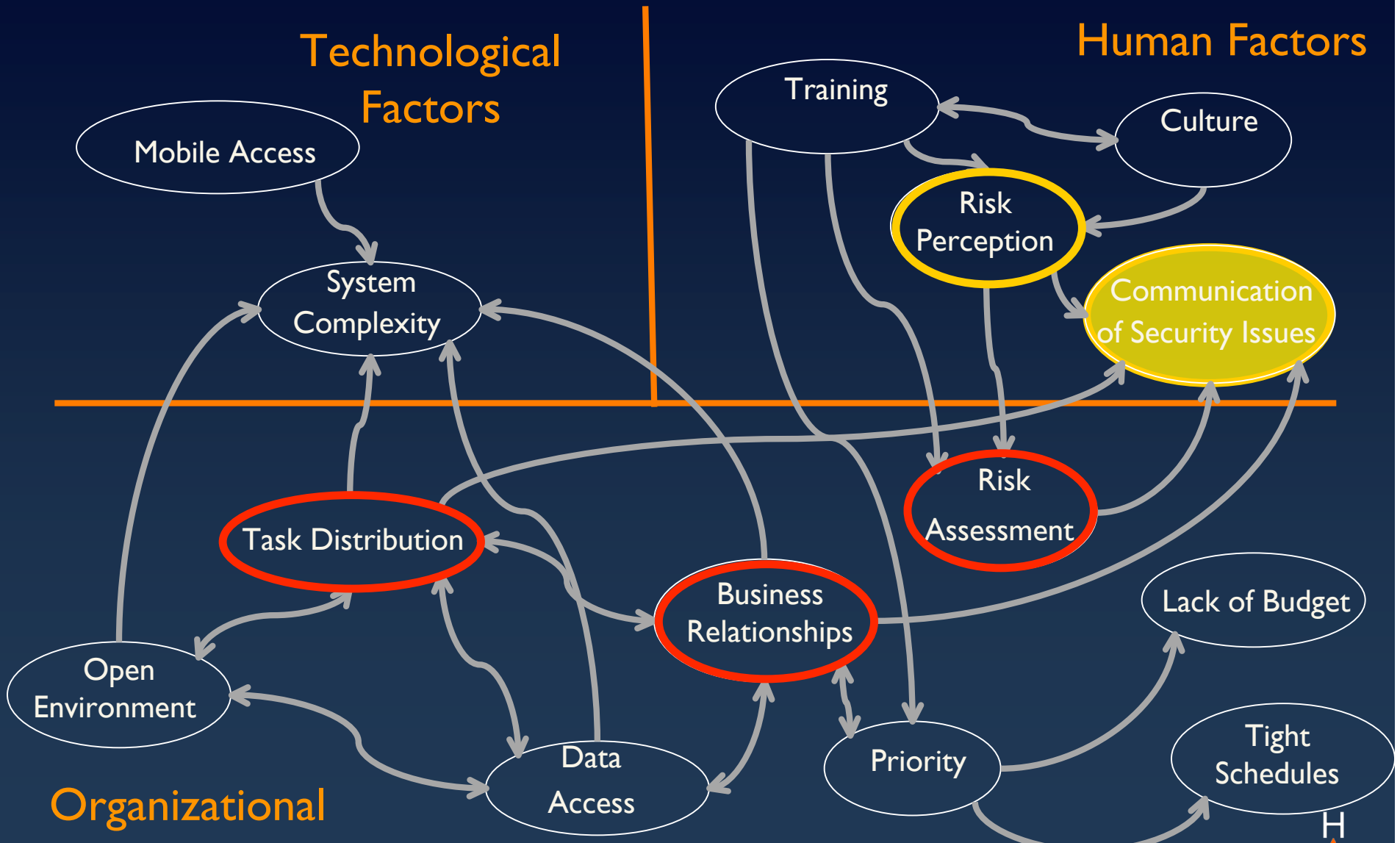
System Complexity

A typical network could have firewalls, DMZs, proxies, switches behind the firewall, routers in front of the firewalls, mail servers and not enough people to look after the overall security of these interconnected devices

Mobile Access

Mobile user access makes it challenging to secure resources

Model of Challenges



Summary

- We provide an integrated framework of the different human, organizational, and technological challenges
  - High interplay of human, organizational and technological challenges
- Framework intended as a guide to support identification of limitations to implementing security

Project Overview

- Field Study
- Analysis & Model Development
  - SP vs.. IT
  - Challenges
  - Interactions
  - Errors
  - Tasks & Tools
  - Management Model
- Guidelines for the Design of Techniques
- Validation of the Results

Interactions

- Research Questions:
  - When and how do security practitioners interact with other stakeholders?
  - What tools do they need to interact effectively?
  - What factors are responsible for miscommunications?
- Motivation:
  - Little related work on how security practitioners interact in real contexts within their organizations

Results


Perform / respond to security audits
Educate and train other employees
Mitigate new vulnerabilities
Design / revise security services
Solve IT security issues of end users
Respond to security incidents
Implement security controls
Develop security policies
Coordinate / Cooperate / Collaborate
IT specialists
Auditors
Organization's committees
IT vendors
End users
Other Organizational units
Managers /executives
External organizational specialists

Tools used during interactions

- Communication:
  - Email
  - Text
  - Incident tracking system
  - Phone, video chat
- Nessus (vulnerability visualization)
- McAffee ePolicy Orchestrator

Recommendations to Improve Tools

- Decrease complexity of interactions
- Support SPs in knowledg
- Flexible repor
- Integration of secu ls
- Reduce communication overhead

e.g., support to interpret om els

e.g., knowledge management ools for policy

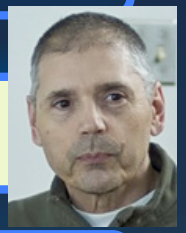
e.g., automatic tailored report generation

Summary

- Analysis shows that SPs work in a complex environment:
  - they not only perform security-specific tasks, but also interact with stakeholders with different backgrounds and needs
- We provide guidelines to improve tools

Results

- Field Study
- Analysis & Model Development
  - SP vs.. IT
  - Challenges
  - Interactions
  - Errors
  - Tasks & Tools
  - Management Model
- Guidelines for the Design of Techniques
- Validation of the Results



Theme: Errors

- Research Question:
  - *What leads to errors in security processes?*
- Motivation:
  - Breakdowns during ITSM can put organizations at risk
  - To reduce breakdowns, we need to understand the causes

Terminology

- Error:

  "*a failure of a structure or process is an indication of error only to the extent that it prevents maximizing the outcomes of interest to the patient*"
  [hofer]

- IT security:
  - the patient = organization
  - Error = security practices that do not maximize outcomes of interest, i.e., *sub-optimal situations*

Suboptimal Situations

Distributed and complex nature of IT security management

Suboptimal situations, i.e., errors

- Busby's framework for errors in a distributed system that includes:
  - Cues: an occurrence which ``*participants use to determine when to act and how to act*''
  - Norms: rules of some sort that help make the participants' subtasks consistent with each other
  - Transactive memory: is a type of mutual understanding, in which people in a group mutually know who is responsible for what
- Errors arise as a result of breakdowns in mutual understanding, cues, norms and transactive memory

Field Study

Analysis & Model Development

Guidelines for the Design of Techniques

Validation of the Results

- SP vs.. IT
- Challenges
- Interactions
- Errors
- Tasks & Tools
- Management Mode

Putting It All Together

- Complexity of IT security management has been a common thread
- Each of our research themes has contributed to community's understanding of security professionals
- Our research has provided a set of guidelines for tool refinements and directions for future research

Future Challenges

- How to create testable models to validate and extend findings?
- How to transform guidelines into concrete tool refinements?
- How to evaluate the success of tool refinements given the complex and distributed nature of ITSM?

Thank-you for your attention!

Web: www.hotadmin.org

Email: kmuldner@ece.ubc.ca