HOT Admin

_Human, Organization, and Technology_ Centred Improvement of IT Security Administration

Konstantin Beznosov, Sidney Fels, Lee Iverson
University of British Columbia

Brian Fisher
Simon Fraser University
Who’s Konstantin Beznosov

- **Education**
  - B.S. in Physics (1993), Novosibirsk State University

- **Experience**
  - Assistant Prof., Electr. and Comp. Egn., UBC (2003-present)
  - Directs Laboratory for Education and Research in Secure Systems Engineering (LERSSE)
  - US industry (1997-2003): end-user, consulting, and software vendor organizations

- **Contributed to**
  - OMG
    - CORBA Security revisions
    - Resource Access Decision
    - Security Domain Membership Management
  - OASIS
    - eXtensible Access Control Markup Language v1.0
Hypothetical Example

ABC Inc.
large company
with 5 divisions

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

1. turn MIME (S/MIME) encryption on
2. enable S/MIME encryption for the user
3. set alpha-numeric rules:
   - Cert. Status Cache Timeout
   - Cert. Status Maximum Expiry Time
   - FIPS Level
   - S/MIME Allowed Content Ciphers
   - Trusted Certificate Thumbprints
4. Set to False
5. Allow Other Email Services
6. Set to True:
   - Disable Email Normal Send
   - Attachment Viewing
   - S/MIME Force Digital Signature
   - S/MIME Force Encrypted Email
   - Disable Invalid Certificate Use
   - Disable Revoked Certificate Use
   - Disable Stale Status Use
   - Disable Untrusted Certificate Use
   - Disable Unverified Certificate Use
   - Disable Unverified CRLs
   - Disable Weak Certificate Use

Total 19 steps!
It’s Not All!

- Now do (most of) the same for other senior managers
- Now do the same on other four servers
- Hard
  - Which of 140 rules need to be set and how?
  - How to remember the right values?
  - How to make sure these are the right values?
  - How to make sure no error was made?
Obvious Limitations of the GUI

- Some interrelations can easily be confused
  - Five rules on public key
    - disable sending of messages encrypted with "Invalid," or "Revoked," or "Untrusted," or "Unverified," or "Weak" certificates
    - Can a certificate have more than one status, e.g., "Weak" and "Unverified"?
    - What is the result of applying more than one of these rules to the same certificate?
    - Which one overrides others, and in what circumstances?

- Difficult to determine the results of changes
  - with the "FIPS Level" = "2"
    - the values of 8 other rules ("Password Required," etc.) are automatically forced to specific values.

- Miss-grouped commands may cause confusion
  - Maximum Security Timeout + Non-Grouped Device-Only
Another Example: Enterprise Authorization Servers
classical access control solution

Access Matrix

<table>
<thead>
<tr>
<th></th>
<th>Domain 1</th>
<th>Domain 2</th>
<th>Domain 3</th>
<th>File 1</th>
<th>File 2</th>
<th>Process 1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain 1</td>
<td>*owner control</td>
<td>*owner control</td>
<td>*all</td>
<td>*owner</td>
<td>*read</td>
<td>*write</td>
</tr>
<tr>
<td>Domain 2</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*read</td>
<td>*write</td>
</tr>
<tr>
<td>Domain 3</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>*owner</td>
</tr>
</tbody>
</table>

subjects
Have access to objects

objects
To be protected
enterprise-scale security server
everything starts with simple tree-like structure
then continues with simple forms to fill out ...
... or select
but the mental model is complex
... and even more ...
... complex
hard to map policies to models
so what?

- steep learning curve
- hard to fit real world into the model
- easy to make costly mistakes
  - “friendly” DoS
  - inadvertent hard to catch config. vulnerabilities
- hard to test
  - expensive to test required scenarios
  - no “what if” scenarios to test before changing
  - hard to perform complete testing
- motivates users and admins to circumvent security

- revenues in security administration software:
  - $1B in 2003
  - $1.6B by 2007

Who is Security Administrator?

- Security administrators
  1. configure, maintain, test and install the technology used to enforce an organization’s security policy
  2. respond to and recover from malicious actions and attacks
  3. administer others’ systems or infrastructures
- end users, power users, administrators
administrators in the epicentres

Human

Organizational

Technological
approach

human-centred

organization-centred  technology-centred
HOT Admin project overview

- **purpose**
  1. evaluation methodology for sec. admin. effectiveness
  2. guidelines and techniques to design sec. admin. tools

- **problem addressed**
  - conflict of human, organizational, and technological forces

- **approach**
  - resolve the conflict through harmonizing the forces

- **work plan (3 years)**
  1. pilot studies to fine-tune the methodologies
  2. field research
  3. development of models
  4. design of techniques and methodologies
  5. validation and evaluation of the project’s key results.

- **team**
  - Beznosov (security), Fels (interfaces), Iverson (collaborations), Fisher (interaction)
purpose

1. methodology for evaluating the effectiveness of the existing IT security administrative tools

2. guidelines and techniques to systematically design effective technological solutions to aid security administrators

3. train graduate students
human-centred

better means for

1. visualizing the state of the security mechanisms

2. providing feedback to security admins
   - “what if” scenarios
   - safe staging playgrounds
   - tests of properties of the security state

3. support for cognitive models of system security
organization-centred

- patterns of communication between different parts of the organization and admins
- offload certain tasks from the admins
technology-centred

accommodate security technology to human and organizational needs

possible examples

- self-administration
- domain-specific access control models and languages
- flexible and reconfigurable policy engines
In 3 years

1. **pilot studies** to fine-tune study plans
2. inventories and an initial analysis through **field studies** with industry
3. development of **models**
   - human, organizational, technological
4. design of **techniques** and **methodologies**
5. **validation and evaluation** of the project’s key results
   - sample admin tools
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., inform. systems
- collaboration infrastructures
Current Status

- Got funding
  - Natural Sciences and Engineering Research Council (NSERC) - $459K

- Got support
  - SAP
  - Entrust

- Getting students
- Getting participants
- Designing studies
project summary

- purpose: develop
  1. tool evaluation methodology
  2. tool design guidelines and techniques

- problem
  - conflict of human, organizational, and technological forces

- approach: resolve the conflict through harmonizing the forces

- work plan (3 years)
  1. pilot studies
  2. field research
  3. models
  4. techniques and methodologies
  5. validation and evaluation

- team
  - Beznosov (security), Fels (interfaces), Iverson (collaborations), Fisher (interaction)
  - + 5 graduate students
We Want You

For HOT Admin!

hot-admin-info@ece.ubc.ca
if your organization participates

we’ll provide:

1. analysis of the organizational environment
2. inventory of the technologies
3. inventory of the conflicts of forces
4. common types of errors

- contact project members
if you want to provide feedback

- workshops with industry partners
- review results
- contact project members
Questions please

http://lersse.ece.ubc.ca/
tiki-index.php?page=Project_HOT-Admin