Why (Managing) IT Security is Hard and Some Ideas for Making It Easier

Konstantin (Kosta) Beznosov

Laboratory for Education and Research in Secure Systems Engineering
Department of Electrical and Computer Engineering
University of British Columbia, Canada
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 (XACML) v1.0
University of British Columbia

founded in 1908
ranked among the world top
• 40 institutes, by the Shanghai Jiao Tong University
• 27 universities, by Newsweek magazine in 2006
• 38 universities, by the Times Higher Education Supplement in 2005
airplanes vs. cars

- flying is fast
- driving is slow
- why isn’t everybody flying?
IT Security is Critical
IT Security is Costly

organizations worldwide spent in 2007

$1.55 trillion on IT
7-9% on IT security

$108 billion

Forrester Research

Cyber crime market worldwide

$105 billion

John Viega, McAfee
why aren't secure systems everywhere?

almost completely insecure, or “secure” but

- too expensive and error-prone to build
- too complex to administer
- inadequate for real-world problems
- forever

examples
what can be done about it?

improvements towards

1. inexpensive and error-proof to build
2. effective and inexpensive in administration
3. adequate for problem domains
4. easy and inexpensive to change and integrate
Outline

• HOT Admin
• JAMES
• SQLPrevent
HOT Admin

a broad empirical study of IT security practitioners and their environment
HOT Admin: Human Organization and Technology Centred Improvement of IT Security Administration

- **Purpose**
  - Tool evaluation: methodology
  - Tool design: guidelines & techniques

**Work Plan**

- Field study
- Models
- Techniques & Methodologies
- Validation & Evaluation

**Sponsors and Partners**

- Entrust
- NSERC CRSNG
- SAP
Human Organization and Technology Centred

Human Organizational Technological

hotadmin.org
Here are some related websites for: hotadmin.org

Sponsored Links

Claims Administration
Learn about the challenges and how technology can help you
www.ClaimVantage.com

Simplify & Centralize Win
Management tasks are centralized and made simple. Great Admin Tool!
www.softwareshelfdistribution.com

Hot Babes In Your Bed
Loneliness Sucks - Fill Your Life With Hot Babes. Video Example!
www.PickUp101.com

Filipinas look for love
Pretty girls from Philippines look for serious relation worldwide
www.filipinokisses.com

Sexy Russian Babe
Find a Hot Russian Babe Online E-mail Amazing Girls Today!
www.Anastasiaweb.com

Third Party Verification
Automated or Live Agent Turn-key, No Capital Costs
www.intelemedia.com

Red Hot Deals
Update your fall look for less with sweet deals on sexy red boots
www.personalshopper.com

Sizing Guide for MySQL
Free Sizing Guide and Performance Benchmarks for MySQL on Blade
www.mysql.com

Sexy women, jt tinney
jt tinney bikini girls stacey hayes Playboy Model Louise Glover, babes
www.knockoutmag.com

Related Categories

Hot Blonde
Hot Bra
Hot Celebrities
Hot Clothing
Hot Ladies
Hot Legs
Hot Swimsuit
Hot Wallpapers
Hot Asian
Hot Cup
methods summary

• data collection
  • online questionnaire
    • demographics
  • in situ semi-structured interviews
    • two interviewers
  • participatory observations
    • 75 hours in academic organization IT department
    • policy development and IDS deployment

• data analysis
  • qualitative description
    • constant comparison, inductive analysis
    • coding: selective, open, axial, theoretical
industry sectors

36 interviews

16 organizations

- Academic
- Finance
- Insurance
- Scientific services
- Manufacturing
- Retail/Wholesale
- Government Agency
- Telecommunications
- Non-for-profit Organization
- High-Tech
- IT Consulting

Laboratory for Education and Research in Secure Systems Engineering
(lersse.ece.ubc.ca)
findings to date
no security admins!

- system analysts
- application analysts
- business analysts
- technical analysts
- system administrators
- application programmers
- auditors
- IT managers
- security leads
- network leads

```
... what makes me [a security] analyst is that I'm also involved in developing the policies and procedures ... an analyst is also someone who's doing a certain amount of troubleshooting and someone who's, I guess, a little bit more portable in terms of what their daily responsibilities are going to be like."
```
loosely coordinated teams

So what?
security is secondary for those who manage it

“I have a security team that I work with. They don't report to me but I actually work with them and they sort of are represented by the different areas.”

Study Participant
skills they practice

- pattern recognition
- inferential analysis
- use of tacit knowledge
- bricolage
  - Dictionary: “construction or creation from a diverse range of available things”
  - Origin: mid 20th century: French, from bricoler ‘do odd jobs, repair.’

So what?
- finding gaps in tool support
- tool improvement
- new usability testing methods
For more information:
technological factors

- Mobile Access
- System Complexity
- Vulnerabilities

organizational factors

- Task Distribution
- Open Environment
- Data Access

human factors

- Training
- Culture
- Risk Perception
- Communication of Security Issues
- Risk Assessment
- Priority
- Lack of Budget
- Tight Schedules

Interactions During Incident Response

Managers
- Coordinate next steps during the investigation
- Ask SP to take action on alarms

External IT organizations
- ISPs/ICP administration
  - Monitor Internet
  - Provide security consultancy
- Share security knowledge (community of practice)

Security practitioners (SP)
Respond to security incident

Notifications
Requirements
Discussion of next steps

IT specialists
- Administrate network or systems
- Administrate data bases
- Forward alarms

Notifications
Requirements
Analysis of the incident

Other Stakeholders
- Redefine product
  - Contact clients or end-users
  - Revise contracts with customers

Notifications
Requirements
Discussion of action plan

End-Users
- Experience security incident
  - Suspect of a security incident

Notifications
Requirements
selected project publications


• R. Werlinger, K. Hawkey, K. Beznosov “Security practitioners in context: Their activities and collaborative interactions” presented at Work in Progress poster session of the ACM SIG CHI conference, April 5-10, 2008, Florence, Italy.
JAMES

flooding and recycling authorizations
departing assumptions

- processor resources virtually free
- commodity computing most cost-effective
- network bandwidth virtually unlimited
- human time/attention expensive
a typical authorization architecture

also known as request-response paradigm
applied by IBM Access Manager, Entrust GetAccess, CA SiteMinder, etc.
request–response paradigm

+ re-use of authorization logic
+ consistent policy enforcement
+ lower admin overhead

- reduced availability
- increased latency
- reduced scalability
addressing the problem

- publish-subscribe
- active recycling
- speculative precomputing

authorization requests

authorization responses
secondary and approximate authorization model (SAAM)

1. reuse previous responses (precise recycling)
2. infer approximate responses (approximate recycling)
SAAM summary

- **basic elements**
  - authorization requests <s, o, a, c, i>
  - authorization responses <r, i, E, d>

- **responses can be**
  - primary or secondary
  - precise or approximate

- **secondary decision point**
  - implemented at PEP
  - uses primary to compute secondary
  - can be safe and/or consistent
selected project publications

• SAAM for RBAC


• SAAM for Bell-Lapadula


• Distributed SAAM


SAAM_{RBAC}: SAAM for RBAC

- Users
- Roles
- Sessions
- Ops
- Obs

- user assignment
- role hierarchy
- permission assignment
- user_sessions
- sessions_roles
- permissions
improvements in availability

100 subjects, 1000 objects, 50 roles

![Graph showing improvements in availability](image)
the impact of various system parameters

- Total users
- Deny responses
- Total roles
- Roles per user
- Roles per permission
- Request distribution

Laboratory for Education and Research in Secure Systems Engineering (lersse.ece.ubc.ca)
Qiang Wei

Matei Ripeanu

Jason Crampton
Information Security Group at Royal Holloway University of London

Kosta Beznosov
SQLPrevent

Effective Dynamic Detection and Prevention of SQL Injection Attacks
Without Access to the Application Source Code
1. Cross Site Scripting
2. SQL Injection
3. Malicious File Execution
4. Insecure Direct Object Reference
5. Cross Site Request Forgery (CSRF)
6. Information Leakage and Improper Error Handling
7. Broken Authentication and Session Management
8. Insecure Cryptographic Storage
9. Insecure Communications
10. Failure to Restrict URL Access

source: http://www.owasp.org/
how SQL injection attack (SQLIA) works

HTTP Request

POST /prodcut.aspx HTTP/1.1
product_id=2 ; SHUTDOWN

Web Application Program Logic

"SELECT * FROM product WHERE id="+ request("product_id")

SQL Statement

SELECT * FROM product WHERE id=2 ; SHUTDOWN
Resulted SQL Statement: sql

Update books set book_name='UPDATE', price=1000 WHERE book_id=123

Tainted Data must only appear in literal
### Performance Overhead

<table>
<thead>
<tr>
<th>subject</th>
<th>detection</th>
<th></th>
<th>prevention</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Avg</td>
<td>Std Dev</td>
<td>Avg</td>
<td>Std Dev</td>
</tr>
<tr>
<td>Bookstore</td>
<td>0.8</td>
<td>0.4</td>
<td>2.7</td>
<td>1.0</td>
</tr>
<tr>
<td>Employee</td>
<td>1.3</td>
<td>0.7</td>
<td>3.1</td>
<td>1.1</td>
</tr>
<tr>
<td>Classifieds</td>
<td>1.0</td>
<td>0.4</td>
<td>2.6</td>
<td>0.8</td>
</tr>
<tr>
<td>Events</td>
<td>2.1</td>
<td>0.6</td>
<td>2.7</td>
<td>1.2</td>
</tr>
<tr>
<td>Portal</td>
<td>1.7</td>
<td>0.4</td>
<td>2.0</td>
<td>0.7</td>
</tr>
<tr>
<td><strong>Average</strong></td>
<td><strong>1.4</strong></td>
<td><strong>0.5</strong></td>
<td><strong>2.6</strong></td>
<td><strong>0.8</strong></td>
</tr>
</tbody>
</table>
SQLPrevent with dynamic taint analysis

• Reduces false positives and false negatives
• Imposes low performance overhead
• Requires no access to application source code
• Enables easy deployment by two config. changes
project team

San-Tsai Sun

Kosta Beznosov
summary

Why (Managing) IT Security is Hard

• HOT Admin

Some Ideas for Making It Easier

• JAMES
• SQLPrevent