



THE UNIVERSITY OF BRITISH COLUMBIA

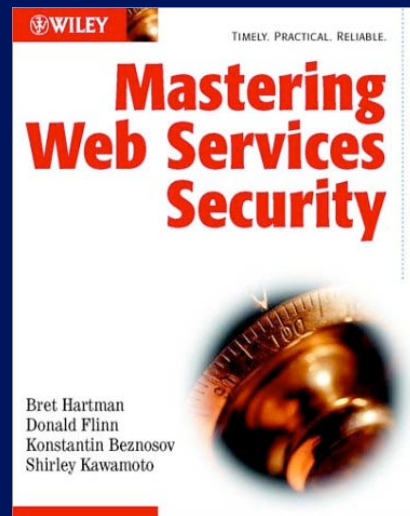
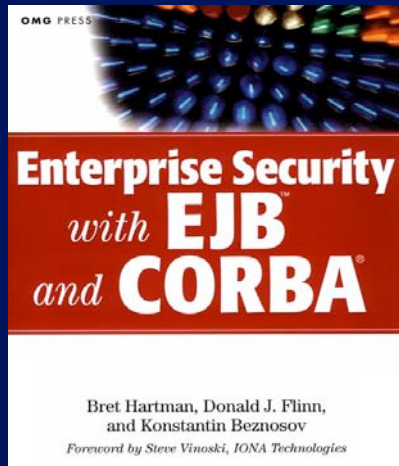
Usable Security: Quo Vadis?

Konstantin (Kosta) Beznosov

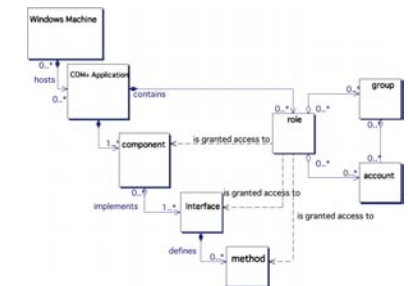
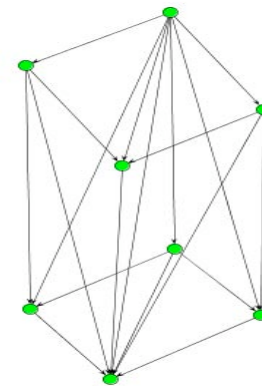
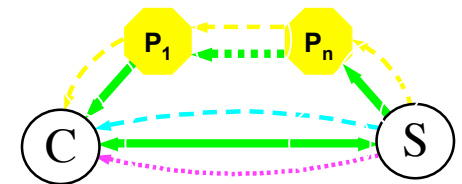
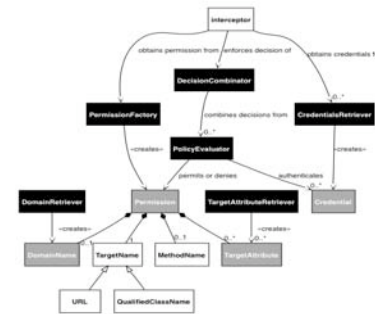
Laboratory for Education and Research in
Secure Systems Engineering
lersse.ece.ubc.ca

Electrical and Computer Engineering

I'm a security engineering guy who also works in HSI Sec



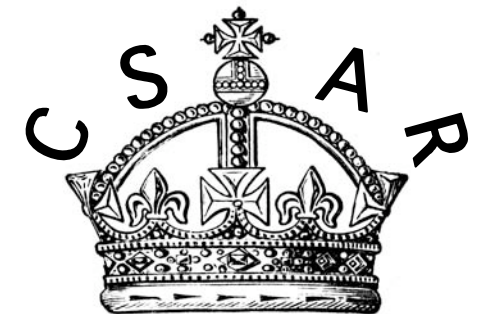
research projects



<http://konstantin.beznosov.net>

<http://lersse.ece.ubc.ca>

H
O T





HCIsec today is up ... for a low hanging fruit

≈ 160 publications
80% in last 7 years



HCIsec Bibliography

The purpose of this web page is to provide a central resource list of published work on human factors in computer security. If you know of any papers that should be added to this list, please let me know. Note that publications of the ACM are also available from the ACM Digital Library.

Usability of Computer Security: A Bibliography contains some overlap. It is arranged by categories and includes some abstracts. It seems to have last been updated in 2000.

Updated 9 April, 2006 by Ponnurangam K.

A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

S A

Mark S. Ackerman, Lorrie Faith Cranor and Joseph Reagle, **Privacy in e-commerce: examining user scenarios and privacy preferences.** Proceedings of the 1st ACM Conference on Electronic Commerce, 1999, Denver, Colorado.

[Author's web page](#)

Mark S. Ackerman, **The Intellectual Challenge of CSCW: The Gap Between Social Requirements and Technical Feasibility.**

[Author's web page](#)



passwords, phishing, messaging important ...



but what about windows?

**if the rest is not secure & usable
locks won't help**



“the rest” is ...

how to

- select
- acquire
- install
- integrate
- configure
- figure it out
- keep up-to-date
- use
- monitor
- notify
- react
- replace

policies & mechanisms

- authentication
- access control
- audit
- detection
- confidentiality
- integrity
- “privacy”
- recovery

scale

- individuals
- groups
- departments
- organizations

device

- cell phones
- PDAs
- pods
- laptops
- desktops
- servers
- grids

expertise level

- novice
- competent
- power
- admins

challenges

HCISec folks

1. make the previous list **green**
2. better **understand** end users
3. **standardized** methodologies, benchmarks, and tools for usability evaluation

	"the rest" is ...	
how to	policies & mechanisms	device
• select	• authentication	• cell phones
• acquire	• access control	• PDAs
• install	• audit	• pods
• integrate	• detection	• laptops
• configure	• confidentiality	• desktops
• figure it out	• integrity	• servers
• keep up-to-date	• "privacy"	
• use	• recovery	
• monitor	scale	expertise level
• notify	• individuals	• novice
• react	• groups	• competent
• replace	• departments	• power
	• organizations	• admins

security folks

1. make **usability evaluation** on par with
 - security analysis
 - performance evaluation

