



THE UNIVERSITY OF BRITISH COLUMBIA

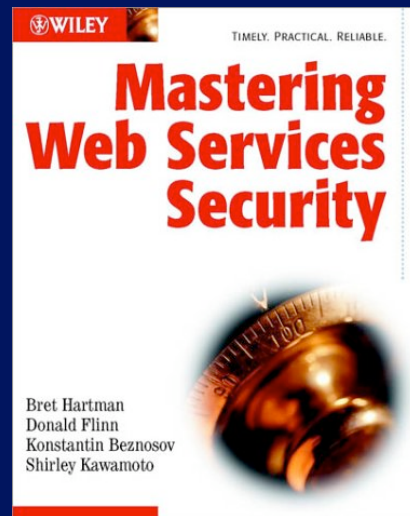
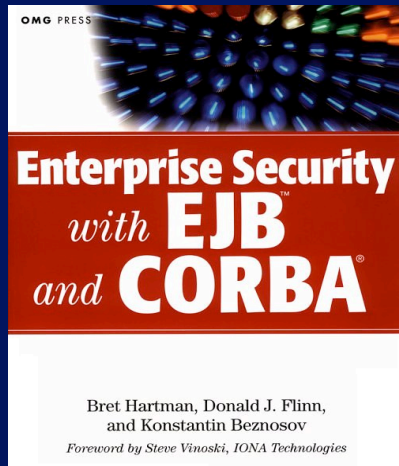
# Usable Security: Quo Vadis?

**Konstantin (Kosta) Beznosov**

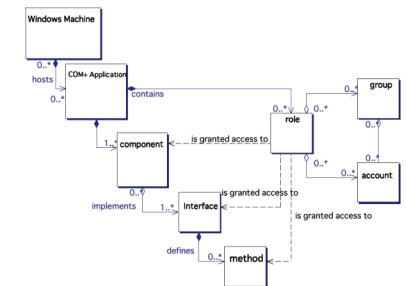
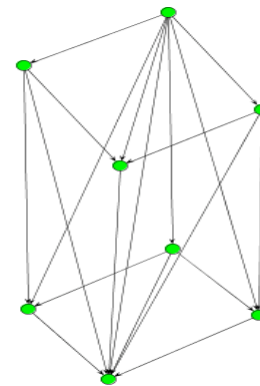
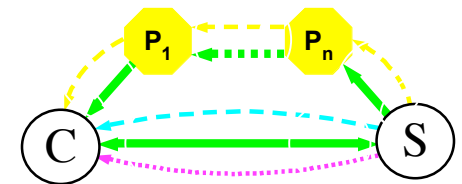
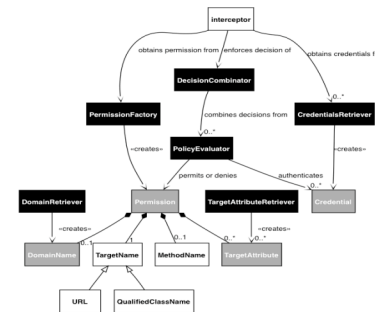
Laboratory for Education and Research in  
Secure Systems Engineering  
[lersse.ece.ubc.ca](http://lersse.ece.ubc.ca)

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 A T





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

≈ 160 publications  
80% in last 7 years



## HCIsec Bibliography

e of this  
work on hu  
that shou  
cations of

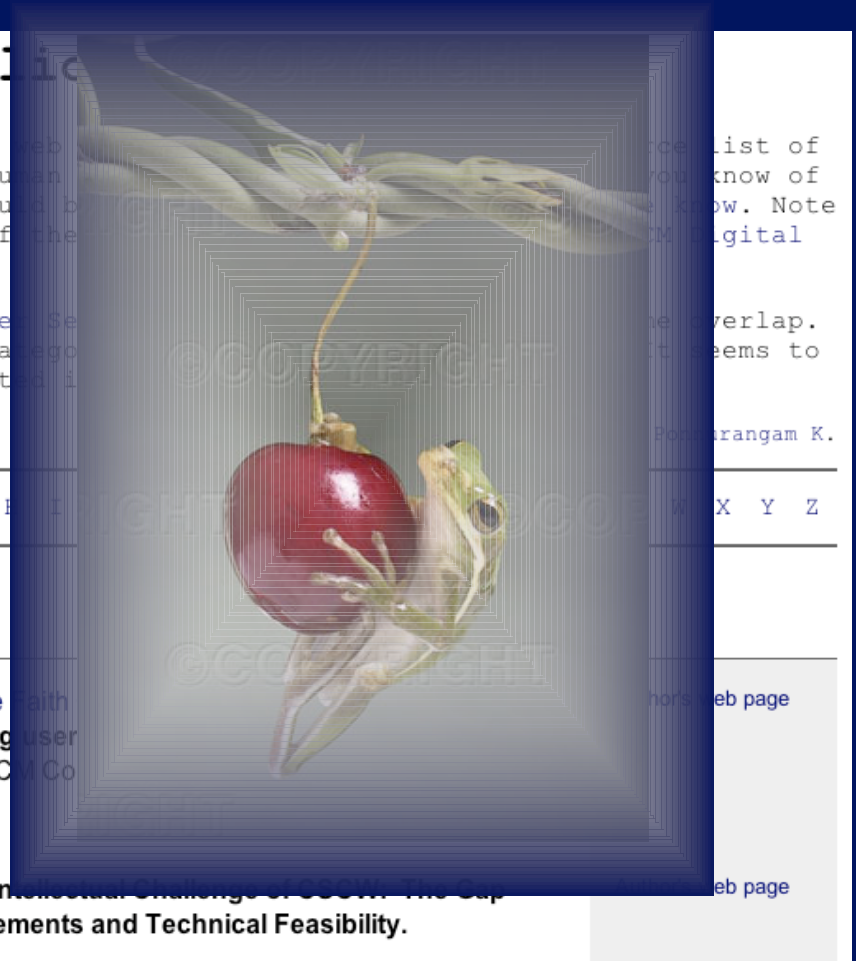
of Compute  
nged by ca  
have last been updat

E F G H I



erman, Lorrie  
e: examining  
s of the 1st AC  
Denver, Colorado.

Mark S. Ackerman, The Inevitable Challenge of Security: The Gap Between Social Requirements and Technical Feasibility.



**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





# Konstantin (Kosta) Beznosov

<http://konstantin.beznosov.net>

Laboratory for Education and Research in  
Secure Systems Engineering (LERSSE)

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