Course Orientation

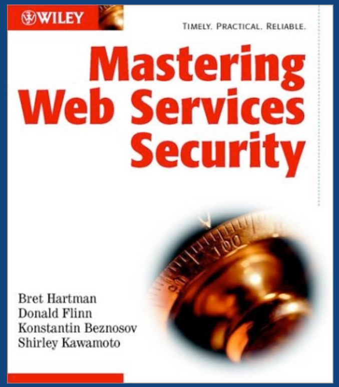
CPEN 542 Cybersecurity

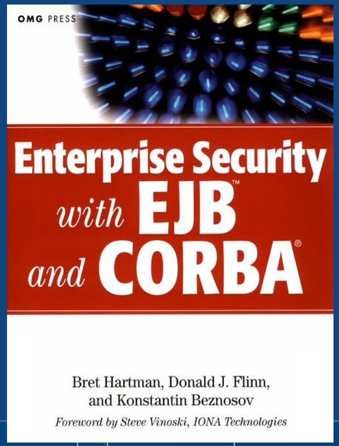
Konstantin (Kosta) Beznosov

Who's Kosta?

(and what is he doing here?)

- CORBA Security SIG
- Industry: Security architect at
  - Baptist Health Systems of South Florida
  - Concept Five
  - (and developer) at Hitachi Computer Products America (HICAM)
  - XACML
- B. Hartman, D. J. Flinn, K. Beznosov, and S. Kawamoto, Mastering Web Services Security, John Wiley & Sons, Inc., 2003.
- B. Hartman, D. J. Flinn, and K. Beznosov, Enterprise Security With EJB and CORBA. John Wiley & Sons, Inc., 2001.




OMG PRESS
Enterprise Security with EJB and CORBA
Bret Hartman, Donald J. Flinn, and Konstantin Beznosov
Foreword by Steve Vinoski, IONA Technologies

research interests

- usable privacy and security (UPS)
- mobile security
- security of online social media/services
- cryptocurrencies
- access control
- middleware and distributed systems security
- network security

introductions

- What is my name?
- Why am I here?
- What do I want from this course?
- Which other courses am I taking this semester?
- What are my interests outside of studies?

intended audience

- new graduate students
  - want to get background in computer security
  - don’t have any such background
  - might or might not do research in security
- senior graduate students
  - same as “new”, plus
  - want to brush up their knowledge of the field with recent papers
  - learn about security aspects other than crypto, hardware, OS
  - want to keep motivated to read on latest research in security
- outstanding senior undergraduate students
  - considering grad school and want to take a grad course

possible topics/themes/units/modules

1. Course Orientation
2. Bootcamp in Computer Security
3. Adversary Models
4. Communication and Network Security
5. Wireless Security
6. Mobile Security
7. Passwords
8. Web Security
9. Smart Meter/Grid Security & Privacy
10. Cloud Computing Security
11. Software Security
12. Usable Security
13. Social Networks Security and Privacy

helpful links

- course web site
  - http://courses.ece.ubc.ca/cpen542/
- syllabus
  - http://courses.ece.ubc.ca/cpen542/syllabus.html
- course forum on Piazza
  - TBD

term paper options

- hands-on
  - usually, either security analysis, or design, or a (measurement) study
  - good for those who is already doing a project that either is related to security, or has a security aspect
  - paper page limit: 10 + references and appendices

- survey paper
  - good for those who is not doing (yet) research related to security
  - allows you to go deep into one particular area of security
  - for larger examples, see
    - ACM Computing Surveys
    - “Systematization of knowledge” papers from recent IEEE Symposium on Security & Privacy (aka, “Oakland” or “S&P”)
  - page limit: 15 + references and appendices
- implementation “paper”
  - pick an open source project on GitHub

hands-on project

- do the project and write the paper in a team of 1-2 students
- format: conference paper + demo
- design, security analysis (a.k.a., “pen testing”), or measurement
- allows you to
  - “double deep” on your ongoing research, or
  - try out an idea for your thesis research with low risk
  - do something that you always wanted to do but did not
- should have
  - clear research value,
  - sound methodology,
  - interesting results
- implementations:
  - approach/tool implementation(s) are required
  - marks for the implementation aspect will be dependent on communicating clearly and concisely
  - what was learned from the implementation, and
  - its novelty or importance to the project
  - prior consultation with the course instructor is strongly recommended

survey paper

- format: conference paper (details TBD)
- allows you to go deep into one particular area of security
- should be “researchy”: demonstrate a solid understanding of the area, insight, e.g., filling in explanatory gaps or smoothly integrating results of several papers
- should include at least
  - an outline and summary of the selected problem(s) and existing solutions in the area;
  - identification and explanations of important recent results and trends; and
  - discussion of important open problems and future research directions.

- see ACM Computing Surveys for larger examples

implementation project

- requirements
  1. pick an open-source project on GitHub
  2. implement a significant security feature/mechanism/ countermeasure
  3. measure performance/usability/scalability/“security”/etc. of your implementation
  4. get your pull request accepted before the mini-conference
- format: conference paper + demo
- allows you to
  - contribute to the community
  - do something that you always wanted to do but did not
- should have
  - clear practical value
  - SE processes in place (e.g., test-driven development)

Questions