Course Orientation

EECE 571B “Computer Security”

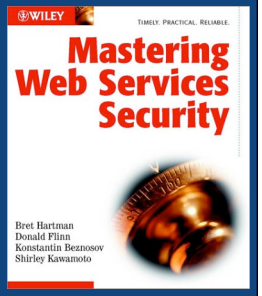
Konstantin (Kosta) Beznosov

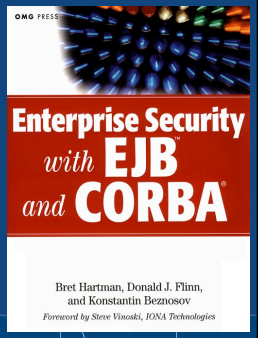
introductions

- What is my name?
- What are my research interests?
- 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?

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.





research interests

- usable security
- web security
- security of online social networks
- network security
- social and business aspects of computer security
- access control
- middleware and distributed systems security

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
  - eager to learn about computer security but missed EECE 412

topics/themes/units/modules

1. Course Orientation
2. Bootcamp in Computer Security
3. Bootcamp in Cryptography (by Prof. Ian Blake)
4. Adversary Models
5. Communication and Network Security
6. Wireless Security
7. Intrusion Detection
8. Password Protocols
9. Authentication
10. On Passwords (and People)
11. Web Security
12. Sybils
13. Usable Security
14. Graphical Passwords
15. Phishing
16. Privacy
17. Mobile Security
18. Cloud Security
19. Social Networks Security
20. Electronic Voting
21. Economics of Security (by Prof. Hasan Cavusoglu)

ece

grading scheme

- Quiz #1 — 18%
- Quiz #2 — 12%

- Term project extended abstract — 10%
- Term project presentation (and demo) — 15%
- Term project paper — 45%

bottom line: project 70% + quizzes 30%

term project options

- hands-on
  - no more than 2 students per project team
  - usually, either security analysis, or design, or a study
  - good for those who is already doing a project that either is related to security, or has a security aspect
  - paper page limit: 15
- survey paper
  - write the paper by yourself
  - 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: 20

hands-on project

- do the project and write the paper in a team of 1-2 students
- format: conference paper + demo
- 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

survey paper

- write the paper by yourself
- 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

ece

important dates

- February 9 — project extended abstract due in the class
- March 6 — quiz #1
- April 5 — quiz #2
- April 11 — project conference papers due by e-mail
- April 13 — course conference (full day, 9-6)

Questions Time!