

<http://www.cs.columbia.edu/~roxana/teaching/CloudMobileS14/>

Cloud and Mobile Security Seminar

Roxana Geambasu ([roxana@cs](mailto:roxana@cs.columbia.edu))

Lecture 1: Class Introduction



Outline

- Introductions
- Administrative overview
- Contents overview
- Example projects



Outline

- Introductions
- Administrative overview
- Contents overview
- Example projects



Who Am I?

- Assistant Professor in the CS Dept. at Columbia
 - <http://www.cs.columbia.edu/~roxana>
- Research areas: distributed systems, operating systems, security & privacy issues
 - Current research focus: addressing data security, privacy, and management challenges raised by cloud computing and mobile devices
- Some accomplishments:
 - Two best paper awards at top conferences
 - Large-scale deployments of research systems to million users
 - Google Fellowships, NSF CAREER award
 - Did my Ph.D. at University of Washington (2011)



Who Are You?

- If class is small: introduce yourselves
- If class is large:
 - How many Master's
 - How many have deep interest in cloud
 - How many have deep interest in mobile
 - How many have deep interest in both
 - How many are interested in security in these systems



Outline

- Introductions
- Administrative overview
- Contents overview
- Example projects



Goals of the Class

1. Broad view of hot research space: security in new mobile and cloud technologies
 - Literature review
2. Discuss, critique, and identify follow-ons to others' research
 - Paper reviews, presentations, and in-class discussions
3. Dive deeply into one unsolved problem and invent solution
 - Semester-long research group project

Grading

- 60%: Course project
- 20%: Paper presentations + reviews (10 + 10)
- 20%: Class participation

For a good grade:

- Be ACTIVE in class!
- Be innovative on the project and do it thoroughly!
- Be insightful in paper reviews!

1. Literature Review

- Will read about 25 papers that **identify or address challenges** raised by cloud computing and mobile devices
- Papers are in a variety of areas:
 - Systems, security and privacy, cryptography, databases
 - However, we focus on **systems** and the application of various techniques from other fields to systems problems
 - Thus, you don't have to fully understand crypto mechanics (for that, take Tal Malkin's class)!
- **Your duties:**
 - **Read** all assigned papers before class
 - **Participate** a lot in class discussions
 - This class will not work if you don't participate in discussions

2. Paper Reviews and Presentations

- Before each class, **submit reviews** for that class's papers
 - Identify strengths, weaknesses, and main points you hope the class discussion will address
- Each class is organized as follows:
 - Instructor provides a **broad view** of the topic of that class
 - Students **present** the papers and lead class **discussions** about them (40 mins/paper: 20 for presentation + 20 for discussion)
- Presentations: 20-25 minutes/presentation
 - All students must present papers (one or two papers/student)
 - If you're doing a complex project, I may waive that for you
 - **Sign up for papers soon** or else we'll assign them to you!
- Everyone must **read all assigned papers** before class

3. Research Project

- Project topic

- ☐ Come up with your own topic
- ☐ Or choose from a list of topics (will post the list soon)
- ☐ Must relate to cloud or mobile and preferably security/privacy
- ☐ Must contain some element of research
- ☐ Must contain a **unique contribution** that's not included in any other of your past or present projects

- Teams of 3 or 4 students (depends on class size)

- **Final deliverables**

- ☐ Research **paper** (10-15 pages)
- ☐ 20-minute conference-style **presentation** (preferably with **demo**)



Project Steps

1. Understand and model the problem
2. Research and understand related work (3-5 papers)
3. Propose some new approach (creativity counts for grade)
4. Implement some parts
5. Evaluate your solution (thoroughness counts for grade)
6. Write up and present your results (writing and talking quality count for grade)

- Do not underestimate the time you must devote to project!
- Work every week, do not procrastinate!
- Important advice: constrain your goals and do them well!



Project Milestones

- Project proposal due 02/10 (0.5 pages)
- Project research plan due 02/24 (1-1.5 pages)
- Project status presentations on 3/24 (5 minute talk)
- Project presentations on 5/05 (15-minute talk)
- Final report due on 5/12 (around 10 pages)

- Meet with TA and/or instructor regularly during office hours to discuss your progress
 - Email and appointments are also valid



CVN Students

- Will replace the class participation and presentation with a 3-page literature review at the end, where you take 5-7 of the papers we've read and discussed how they all fit together.

Staff and Office Hours

- Instructor: Roxana

- Office hours: Tuesdays 4-5pm, CSB 461

- TA: Andrei Papancea

- Office hours: see website

- Web page: reading schedule, project timeline, etc.

- www.cs.columbia.edu/~roxana/teaching/CloudMobileS14

- Please note that the schedule is up for change (only stable w.r.t. the following lecture)



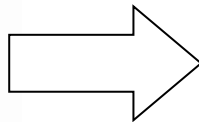
Outline

- Introductions
- Administrative overview
- Contents overview
- Example projects

Trend 1: Cloud Computing and the Web

- Data, applications migrate from **in-house, dedicated, self-managed** environments to **public, shared** clouds
- Cloud computing brings many **advantages**:
 - Universal accessibility to data and applications
 - Less software/hardware management
 - Automatic scaling based on use

In-house infrastructure



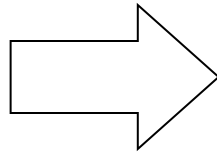
Cloud computing



Trend 2: Small, Powerful, Mobile Devices

- Small, powerful mobile devices are replacing desktops as primary computing platform
- Mobile devices bring important **advantages**:
 - Location-based services, mobile web
 - Constant connectivity, data access, email

Desktop



Small mobile devices



Tech Trends Raise Significant Challenges

- Challenges are numerous and diverse:

- ☐ Security
- ☐ Availability
- ☐ Reliability
- ☐ Scalability
- ☐ Performance
- ☐ Power
- ☐ Cloud isolation
- ☐ Cloud lock-in
- ☐ Small-form device usability
- ☐ ...

- This class: data security, privacy, and management challenges

What's Happening to the Data?

Old desktop world



data

New cloud and mobile world



- Data was centralized
- Data was owned and controlled by the user
- Single user
- Desktop was relatively safe physically

- Data is **fragmented** and **replicated**
- Data is owned and controlled by **untrusted** third parties
- Users **share** cloud infrastructure
- Mobile devices are extremely prone to **theft or loss**



Example Challenges (1/2)

■ Data confidentiality

- How to prevent Facebook, advertisers, mobile thieves, or co-located Amazon EC2 users from accessing your data?

■ Data access control

- How to share Facebook data with only a few people when Facebook only allows one-size-fits-all access control policy?

■ Data access auditing

- How to tell who has accessed your data on Facebook or on a stolen mobile device?

■ Data access privacy

- How to prevent Gmail from knowing whom you're communicating with?



Example Challenges (2/2)

- Data availability

- ☐ How to ensure that your cloud data is replicated enough?

- Long-term data persistence

- ☐ How to ensure that you don't lose your data when you lose a device or when your cloud storage goes bankrupt?

- Data deletion

- ☐ How to ensure that all copies of your Gmail emails are actually deleted when you request that?

- Data management

- ☐ How to organize your data meaningfully when it is scattered across many services and devices?

- ...



This Class

- Identify data security, privacy, and management challenges raised by cloud and mobile computing
 - Review known techniques to address these challenges
 - Understand their limitations
 - Identify common approaches for dealing with challenges
- This is a young & active research space with **no ground truths or perfect solutions**
 - E.g., no one knows if *any* of the previous challenges are solvable
- The class will be research-oriented
 - We may talk about not-so-practical solutions, just to understand what's doable
 - We may talk about practical solutions that do not withstand certain attacks

Class Schedule

02/11	Cloud computing	
02/18 – 02/25		
03/04 – 03/11		
03/25		
04/01		
04/08	Mobile devices	
04/29		
05/06		

Class Schedule

02/11	Cloud computing	Challenges	- Misc challenges such as the ones before; - Side-channel attacks.
02/18 – 02/25		Cryptographic techniques	- Computation-enabled cryptography; - Trusted storage on untrusted infrastructure; - Limitations of crypto techniques for cloud.
03/04 – 03/11		Trusted hardware techniques	- Virtual private clouds; - Trusted incrementers; - Limitations of trusted hardware.
03/25		Distributed trust systems	- Secure multi-party computation; - Threshold secret sharing; - Distributed-trust self-destructing data.
04/01		Auditing and monitoring	- Proofs of retrievability; - Auditing persistence for archival systems.
04/08	Mobile devices		
04/29			
05/06			

Class Schedule

02/11	Cloud computing	Challenges	- Misc challenges such as the ones before; - Side-channel attacks.
02/18 – 02/25		Cryptographic techniques	- Computation-enabled cryptography; - Trusted storage on untrusted infrastructure; - Limitations of crypto techniques for cloud.
03/04 – 03/11		Trusted hardware techniques	- Virtual private clouds; - Trusted incrementers; - Limitations of trusted hardware.
03/25		Distributed trust systems	- Secure multi-party computation; - Threshold secret sharing; - Distributed-trust self-destructing data.
04/01		Auditing and monitoring	- Proofs of retrievability; - Auditing persistence for archival systems.
04/08	Mobile devices	Challenges	- Theft; - Apps leaking data.
04/29		Anti-theft techniques	- Zero-interaction authentication; - Post-theft auditing.
05/06		Data dispersion techniques	- Virtual private clouds; - Trusted incrementers; - Limitations of trusted hardware.



Outline

- Introductions
- Administrative overview
- Contents overview
- Example projects

- 
- Please see CourseWorks document

Next Class

- Topic: Survey of cloud computing challenges
- Readings:
 - **Above the clouds: A Berkeley view of cloud computing**
 - **Hey, you, get off of my cloud: Exploring information leakage in third-party compute clouds**
 - Need two volunteers to present these two papers (otherwise I will name two people myself)
- Assignments:
 - Sign up to present papers (email 2-3 preferences to TA)
 - **First project deadline on 2/10: project proposal (0.5-page description of your project)**



Questions?