

Cybersecurity Research and Online Learning

John Mitchell
Stanford University

Security and privacy

- We are developing a new class of systems with new uses for new communities
- Security and privacy are pervasive concerns, central for this area because
 - Student records are confidential and personal
 - Social networks reveal personal, confidential information
 - Course material may be owned, shared, licensed, recombined, ...
 - Extensive data collection and analysis is part of the revolution

Summer-Fall 2011

- Sebastian Thrun, AI course
 - Udacity platform, controversial publicity
- Fall Stanford courses
 - Jennifer Widom, Databases
 - Andrew Ng, Machine Learning
- Statistics
 - Approx 350,000 registered interest online
 - Tens of thousands completed courses
 - Statement of Accomplishment

Excitement in the news

- Public concern over the cost of education
 - Education debt exceeds credit card debt
- Stanford offerings are
 - Free
 - Available to everyone
- The numbers have been phenomenal
 - More than 1.5 million Coursera users to date

What is Political (System) Legitimacy?

- ⊗ The belief that the system of government is the best one for the country, that it is morally right, proper, and justifiable, that it deserves (voluntary) allegiance
- ⊗ A “moral title to rule”—to command obedience, to tax and draft, to legislate and enforce laws



Maya Adam, Nutrition



Yoav Shoham, Game Theory

Rock-Paper-Scissors

Generalized matching pennies.

	Rock	Paper	Scissors
Rock	0, 0	-1, 1	1, -1
Paper	1, -1	0, 0	-1, 1
Scissors	-1, 1	1, -1	0, 0

...Believe it or not, there's an annual international competition!

Game Theory Online



Stanford Report, October 15, 2012



At Stanford, scholars debate the promises, pitfalls of online learning

Tanner Lecturer and respondents tackle the challenges of preserving the best of higher education while venturing onto new ground.

BY R.F. MACKAY

For the first time in centuries, university administrators and intellectuals are seriously questioning the logic of how we teach and learn, and for the first time, we may actually have the technology to shift the education paradigm. The bad news, according to scholar William G. Bowen, is that there is no quick fix, though clearly technology is a large part of the solution.

Online learning is not just one thing, and it is far from static, he said during his lecture Oct. 11 titled "Prospects for an Online Fix: Can We Harness Technology in the Service of Our Aspiration?" But it is here to stay. He was once a skeptic, he emphasized, and he rarely has visions, but today he's a convert.

"Now is the time" for online learning innovation, he stated at the start of his lecture, but he went on to point to three barriers to implementation: little hard data, no shared software platforms to

L.A. Cicero



Now is the time for innovation in online learning, scholar William Bowen told the Stanford audience.

Tremendous Opportunity

- Evolving technology give us an opportunity to expand and reinvent education at all levels
 - Interactive video: embedded questions
 - 15 min segments, question every 3-5 minutes, auto-graded
 - Automated assessment: quizzes, exercises
 - Can we grade calculus? Software design? English papers?
 - Social networking: online discussion, collaboration
 - Schedule and timeline have huge effect
 - Peer evaluation, reputation rankings
 - Simulated environments:
 - Computer-simulated physics, chemistry, economic phenomena,...

Stanford Report, August 30, 2012

Stanford takes landmark step in online learning, appoints new vice provost

The creation of the Office of the Vice Provost for Online Learning – part of the larger Stanford Online initiative – signals both a restructuring of the university and its dedication to ensuring pedagogical agility and rigor in the face of global, economic and social transformations.

BY STANFORD REPORT STAFF

Stanford University today announced the creation of an Office of the Vice Provost for Online Learning, a landmark step in its commitment to bring new teaching and learning methods to Stanford students – and to students around the world – in response to the requirements and potential of the 21st century.

The first vice provost of the office will be computer scientist John Mitchell, the Mary and Gordon Crary Family Professor in the School of Engineering. Earlier in the year he was named by President John Hennessy to be chair of the Presidential Advisory



L.A. Cicero

SHARE THIS STORY

195

467

12

Recommend

Tweet

Stumble

RELATED TO THIS STORY

» Stanford Online

» John Mitchell

MORE STANFORD NEWS

RECENT

POPULAR

SUBSCRIBE

American West's changing climate spells economic changes, too, according to Stanford symposium

Stanford's newly minted Rhodes Scholars shaped by personal narrative

Some personal history ...



STANFORD COURSEWARE

Social Network based Course Management System

Built summer 2009
with 6 undergrads

Kokosenski
Conner Poppen
Winslow Duong
Chen

Quick Links

Welcome to CourseWare. Here are places you might be interested in:

- [Profile](#)

Course membership

CS157

Logic and Automated Reasoning

Taught by Professor


CS142

Web Applications

Taught by Eric Conner


CS107

Computer Organization and Systems

Taught by Professor


CS109

Introduction to Probability for Computer Scientists


Taught by Professor


Calendar

List	Day	Week	Month			
<< < August 2009 > >>						
Sun	Mon	Tue	Wed	Thu	Fri	Sat
						1
2	3	4	5	6	7	8
9	10	11	12	13	14	15
16	17	18	19	20	21	22
23	24	25	26	27	28	29
30	31					

Today

Notifications

You have a new message from Professor. It reads: (asdasd) To view your messages, click [here](#). To send Professor a message, click [here](#). 

You have a new message from Professor. It reads: (test) To view your messages, click [here](#). To send Professor a message, click [here](#). 

CS157: There is a new [comment](#) on a topic you have been following 

Topics You're Following

Filter ▾

Does anyone know how to find the length of a C-string? resolved
Student

Does anyone know how to structure a for loop in C? pending
Student

Does anyone know how to structure a for loop in C? pending
Student

Does anyone know how to structure a for loop in C? pending
Student

Fully Customizable

[Edit Dashboard Configuration](#)












Current Courses -- Col x

https://courseware.stanford.edu/pg/courses/current

CourseWare Courses Help John Mitchell

My Courses
Current Courses
Archived Courses

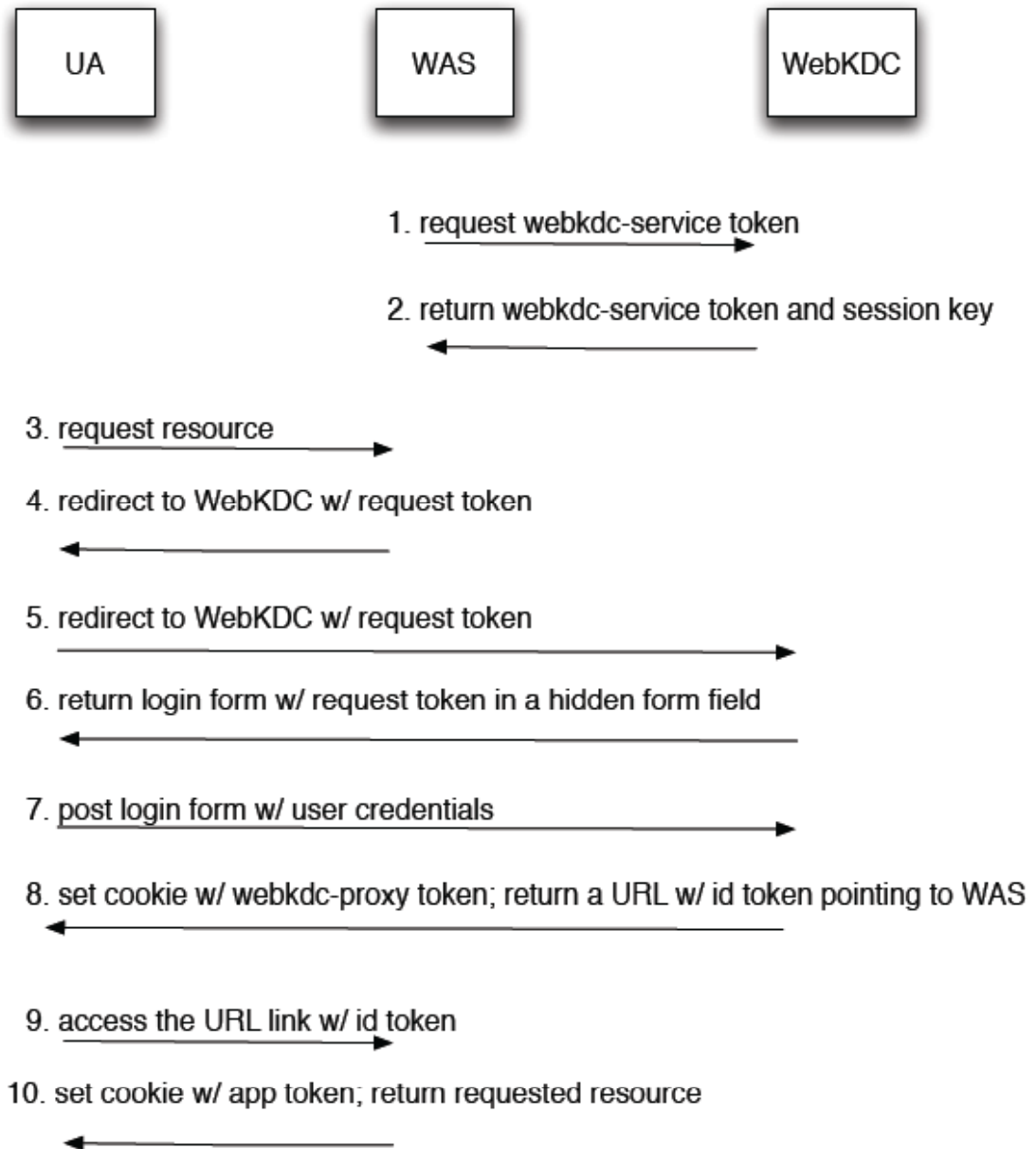
Current Courses

	Bio43: Evolution, Ecology, and Plant Biology (Spring 2012) MWF 11:00am - 12:15pm in Hewlett 200 with Kirill Bersuker, Waheeda Khalfan	Join
	CCC101: CourseWare Crash Course for Beginners (Spring 2012) MW 9:30am - 11:30am in with Task 01	Join
	CME213: Introduction to parallel computing using MPI, openMP, and CUDA (Spring 2012) MW 12:50pm - 2:05pm in 60-120 with Eric Darve	Join
	CS1U: Practical Unix (Spring 2012) Th 1:00pm - 1:00pm in Gates B30 (Pup Cluster) with Sam King	Join
	CS107: Computer Organization and Systems (Spring 2012) MF 12:50pm - 2:05pm in 420-40 with Julie Zelenski	Join
	CS155: Computer and Network Security (Spring 2012) TTh 2:15pm - 3:30pm in Nvidia Aud with Dan Boneh, John Mitchell	Join
	CS181: Computers, Ethics, and Public Policy (Spring 2012) MW 9:30am - 10:45am in Herrin T175 with Steve Cooper, William Rowan	Join
	CSE 441: Advanced HCI: User Interface Design, Prototyping, and Evaluation Part II (Spring 2012) TTh 12:00pm - 1:20pm in University of Washington, CSE 503 with James Landay	Join
	Cognitive Science 102C: Cognitive Design Studio (Spring 2012) TTh 12:30pm - 1:50pm in Peterson 104 with Whitney Friedman, Daniel Frysinger, Professor Hollan	Join
	EE282: Computer Systems Architecture (Spring 2012) MW 11:00am - 12:15am in Gates Hall B01 with Sue George, Christos Kozyrakis, Jacob Barton Leverich, Matthew Murray	Join
	ICS121V: Social Media Toolkit (Spring 2012) Th 9:00am - 10:00am in Online with Burt Lum	Join

University system: WebAuth

- Web-based Single Sign-On protocol
- WebAuth and a similar protocol, Central Authentication Service (CAS), are deployed at over 80 universities worldwide
- We analyzed and improved WebAuth
 - Formal model of the web, using Alloy
 - Found exploitable vulnerability
 - Verified the same vulnerability in CAS
 - Provided and verified practical repair

WebAuth Protocol



WebAuth Attack

UA

WAS

WebKDC

1. request webkdc-service token

2. return webkdc-service token and session key

3. request resource

4. redirect to WebKDC w/ request token

5. redirect to WebKDC w/ request token

6. return login form w/ request token in a hidden form field

7. post login form w/ user credentials

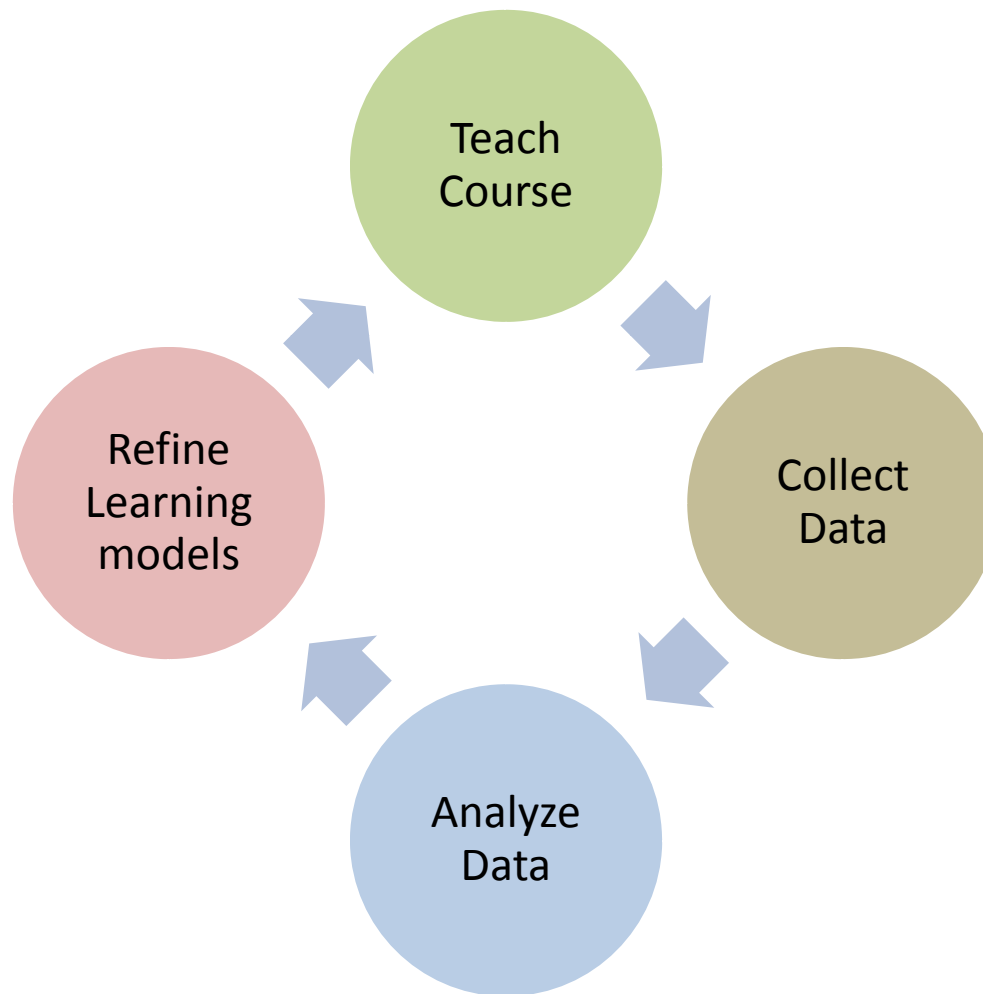
8. set cookie w/ webkdc-proxy token; return a URL w/ id token pointing to WAS

Attacker completes steps 1-8 and induces the user's browser to send message 9

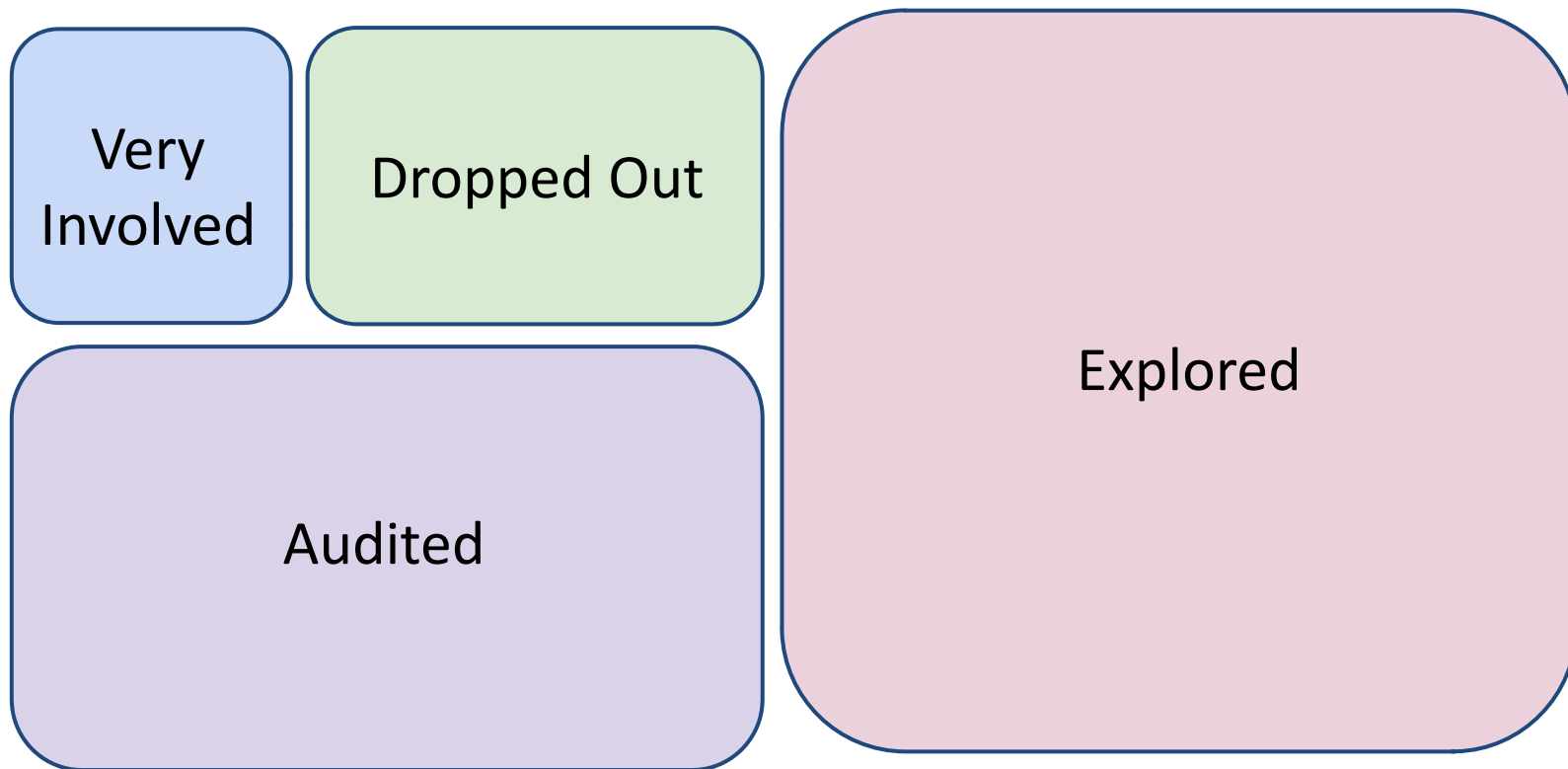
9. access the URL link w/ id token

10. set cookie w/ app token; return requested resource

Learning analytics => “Lytics Lab”

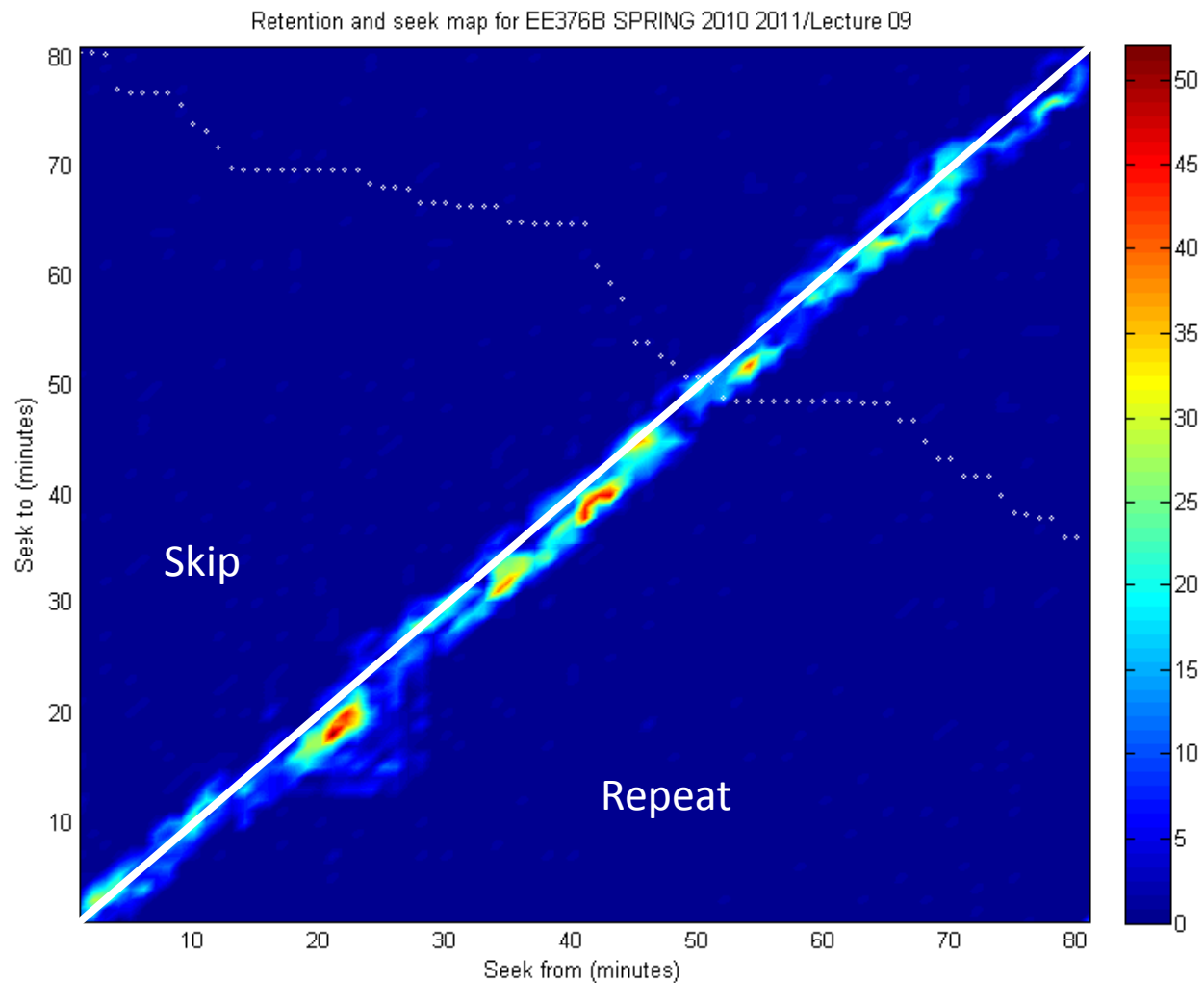


Clustered patterns of engagement



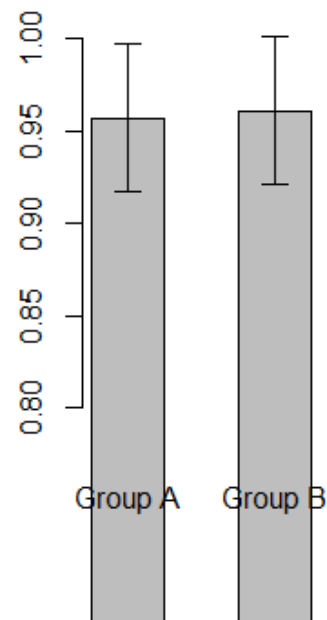
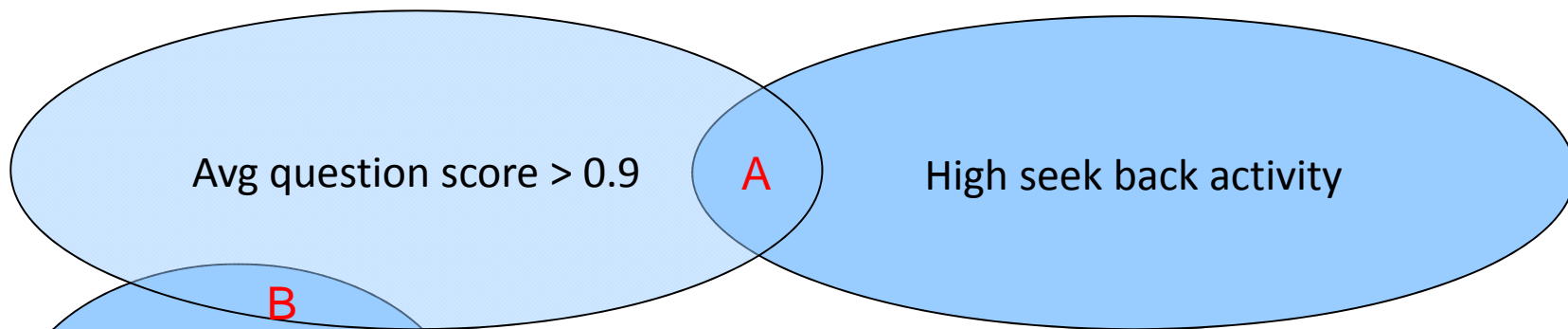
Not including registrants that never watched a video or did a quiz.

Simple Visualization of Seek Data

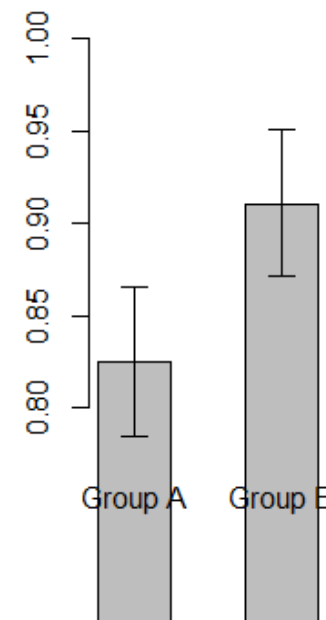


S. Halawa, R. Kizilcec, E. Schneider, and John Mitchell (Stanford University)

Comparison of student groups



Question #1



Question #3

Peer Grading Network

HCI assignment 5

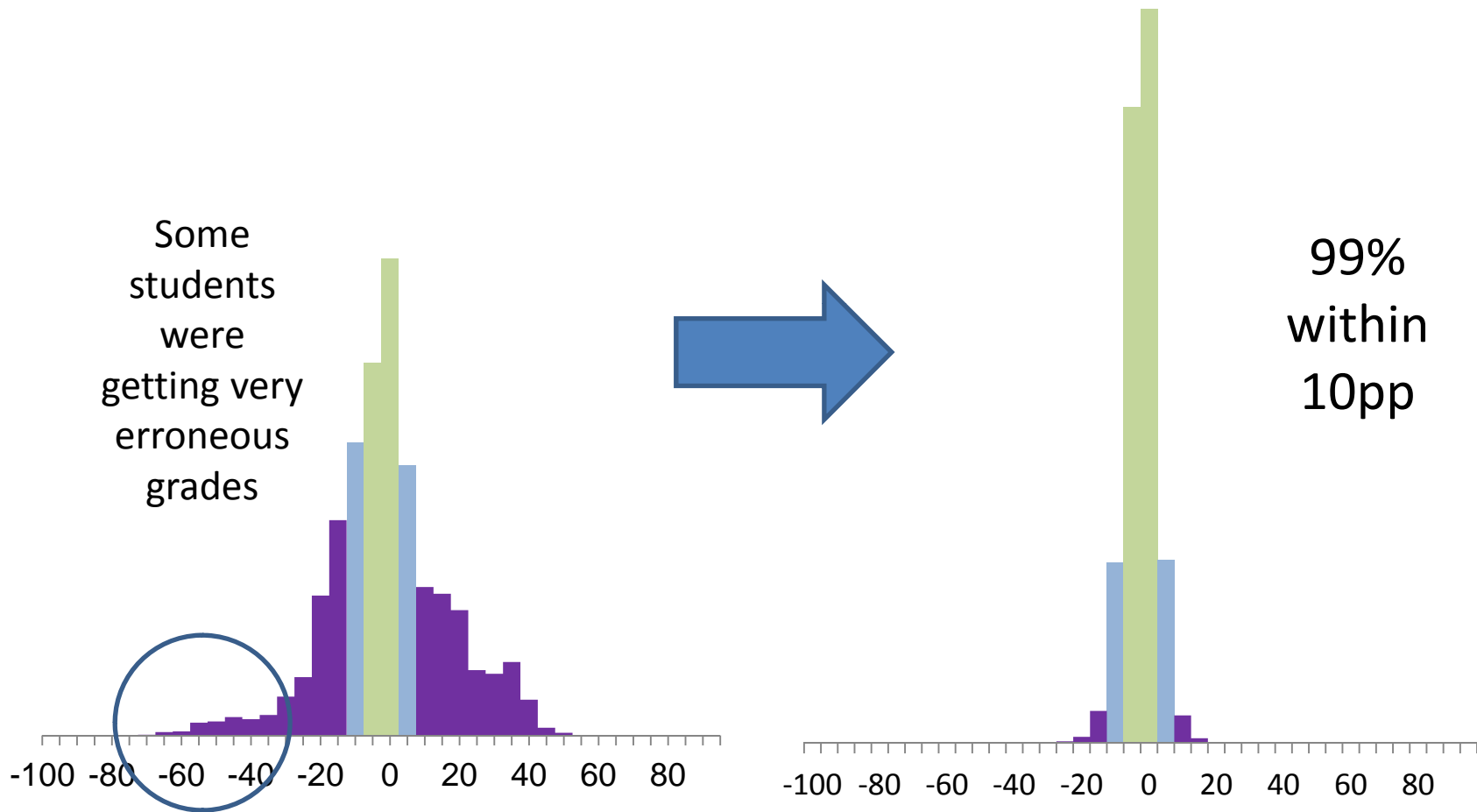
Dummy assignment

One student is highlighted

● student she graded

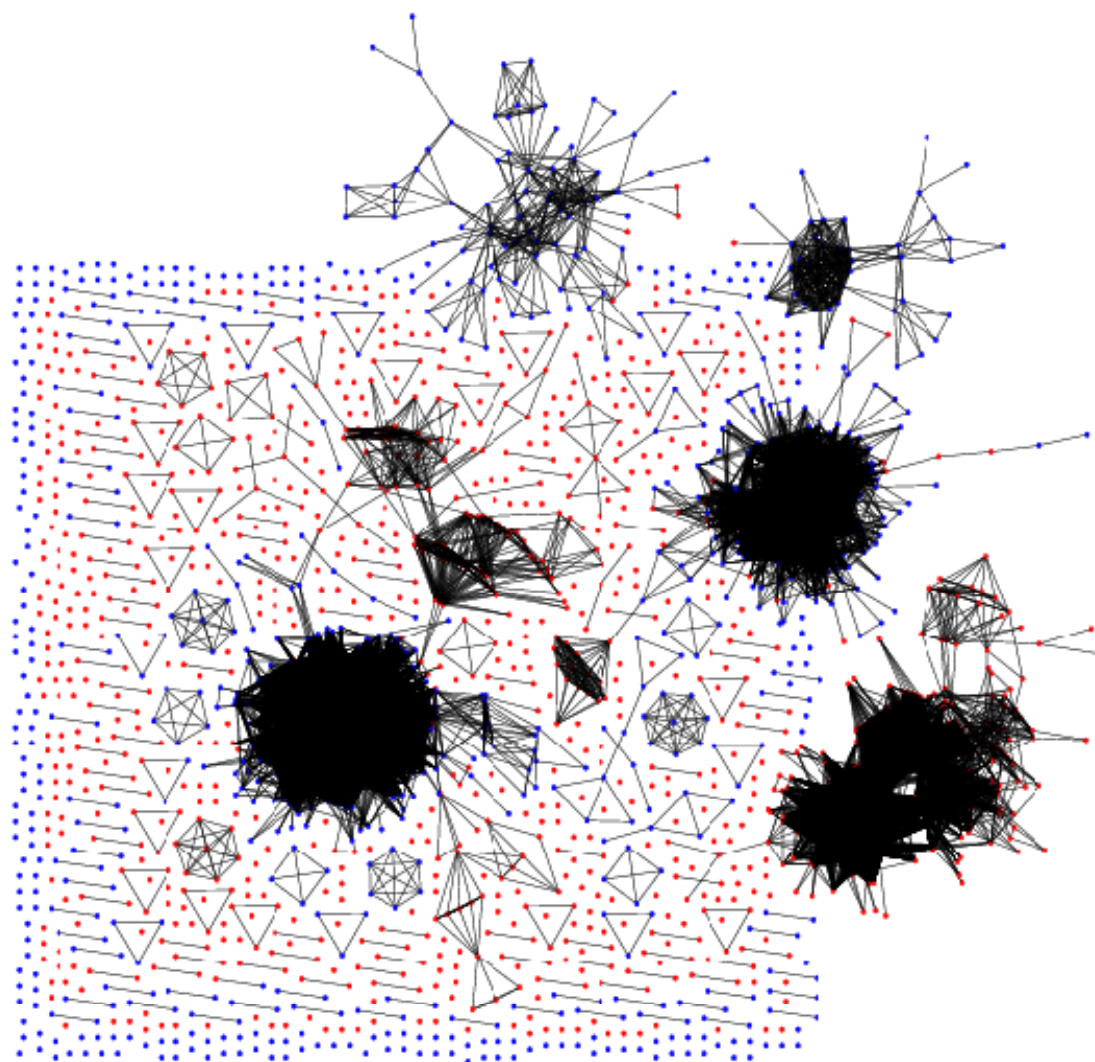
■ student who graded her

Improved Accuracy From Modeling Graders



Corrections involve weighting reliable graders and additive correction for bias.

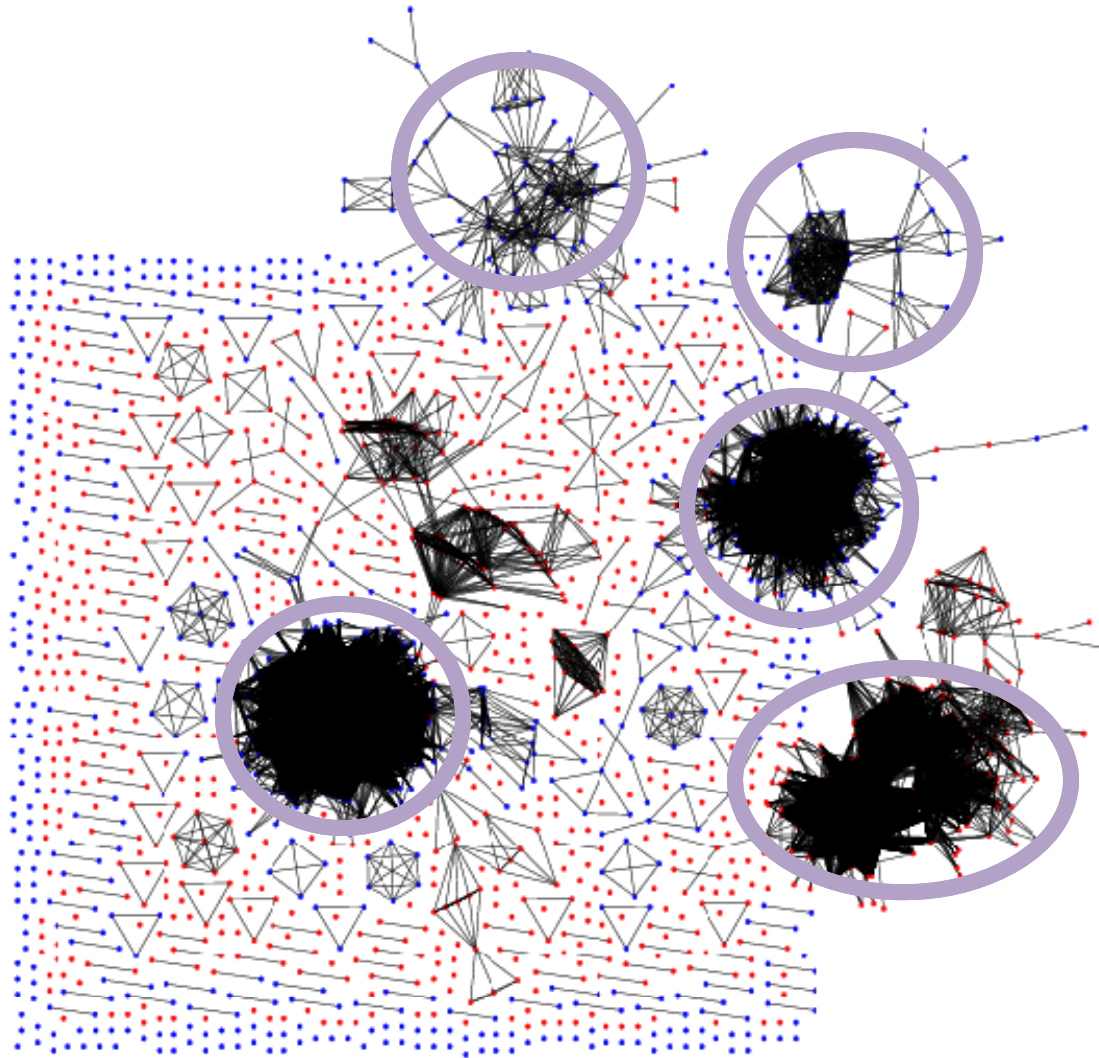
Group ML programs by similarity metric



3000 nodes
shown,
connected if
similar

Red = Incorrect
Blue = Correct

Find Prototypical Solutions



Similar clustering
in CS106A logs of
students solving
their homework

Basic Security Requirements

- Student records are confidential and personal
- Social networks reveal personal, confidential information
- Course material may be owned, shared, licensed, recombined, ...
- Various forms of cheating are pervasive
- Extensive data collection and analysis is part of the revolution

Sample challenges (1)

- User annotation of learning material
 - Traditional cross-site scripting, cross-site request forgery, ... for web applications that allow user input such as executable code (e.g., in programming classes), annotation and modification of content,
- Reputation in group projects, peer evaluation
 - Integrity of reputation mechanisms and robustness against self-maximizing malicious behavior

Sample challenges (2)

- Assessment and stand-alone credentials
 - Can we develop ways of assessing student skills that are more informative to employers than A, B, C, ...
 - How do we make these robust against various forms of “cheating”?
- Data sharing and educational research
 - What anonymization and privacy measures are appropriate?
 - Students may want to demonstrate their knowledge publicly
 - Known attacks on social network graph may apply

Sample challenges (3)

- Beyond the “course”
 - Learning objects can be combined to support hybrid and fully online learning
 - How do we support integrity and provenance in this environment?
 - Should a learning object repository enforce licenses governing combination and reuse?
 - Interesting instance of secure information sharing

Conclusion

- Education is a new frontier for computing
 - Interdisciplinary research area involving new learning models and new technology to support and evaluate them
- New systems \Rightarrow new security requirements
 - Student records are confidential and personal
 - Social networks reveal personal, confidential information
 - Course material may be owned, shared, licensed, recombined, ...
 - Various forms of cheating are pervasive
 - Extensive data collection and analysis is part of the revolution



Unleashing innovation
and creativity in online
learning

[Find Courses](#)

FEATURED COURSES



Introduction to Databases

Starting: Jan 15 2013

This is an introductory course on databases primarily focusing on how databases and



Cryptography II

Starting: Jan 21 2013

Learn about the inner workings of cryptographic primitives and protocols and how to apply

RECENT NEWS

As learning goes digital, big data can guide us
3 days 10 hours ago

Higher education grapples with accreditation in the digital age
1 week 2 days ago