

Cybersecurity Research and Online Learning

John Mitchell
Stanford University

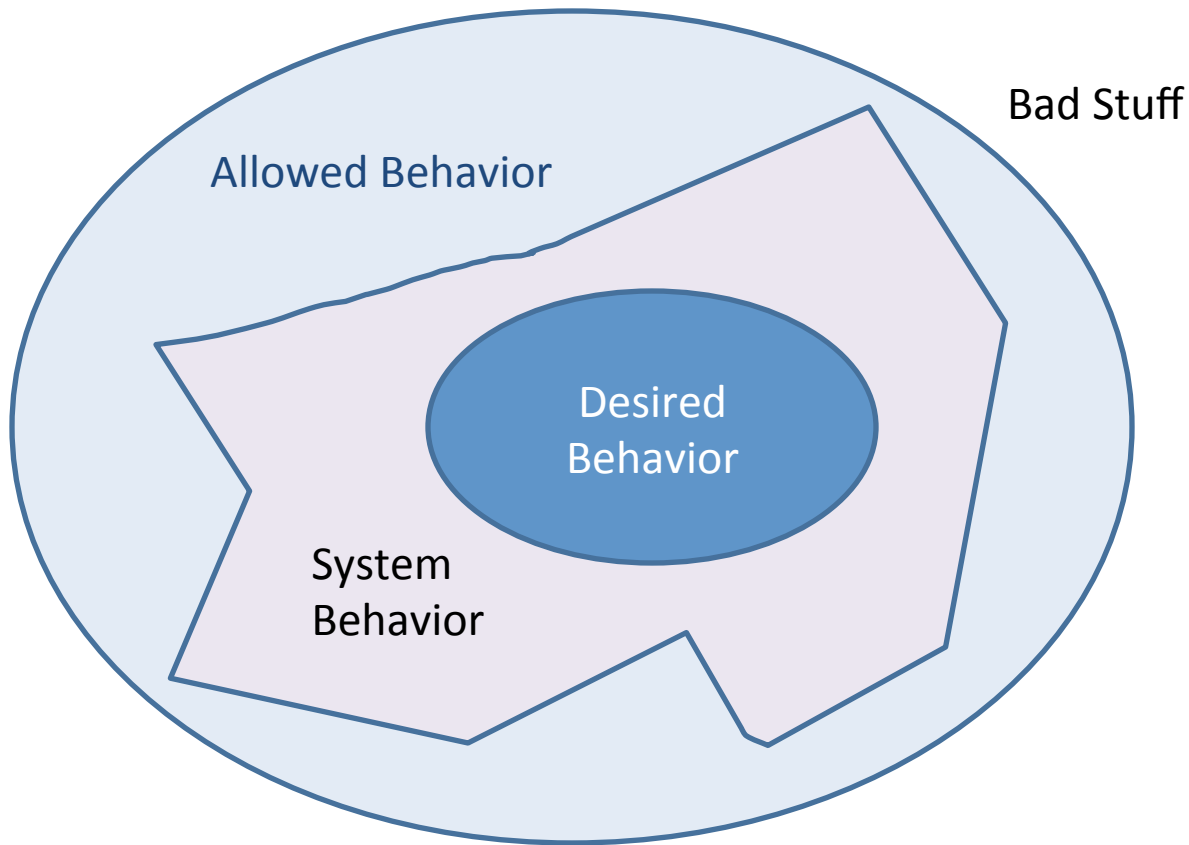
Some context

- Online teaching and learning
 - The announced title for this talk says something about MOOCs – massive open online courses
 - MOOCs are only one part of an emerging revolution
- 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

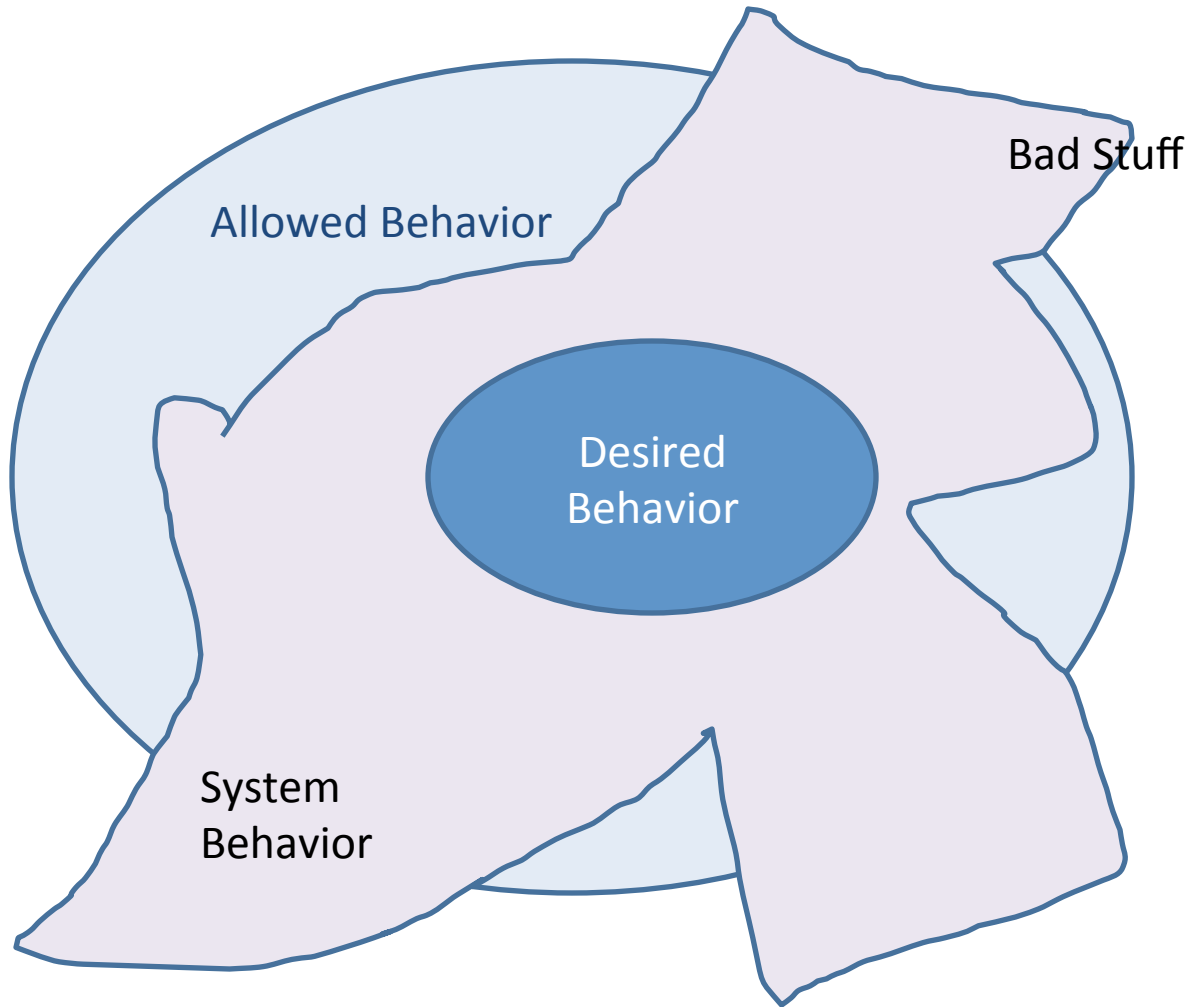
Computer Security

- Allow desired system behavior
 - Users must be able to use system for its intended purpose
- Prevent undesirable behavior (misuse)
 - Adversary must not be able to violate specified security requirements

Computer Security



Computer Security



Online teaching and learning

- Intended users
 - Instructors at producing institution
 - Instructors at other institutions that license content
 - Students, enrolled in course or in self-study mode
 - Educational researchers analyzing data
- Intended functionality
 - Instructors access material, update, customize, ... enter grades
 - Students view course material, participate in discussion, group projects, self-evaluation, peer-evaluation, ... view grades
 - Data collected and made accessible for research

Security

- Adversary
 - Spammer or stalker looking for targets
 - Student who wants to cheat
 - Unauthorized institution that wants to reuse material
 - May have network access, compromised account
- Security requirements
 - Transcript or grades accurately reflect student activity
 - No student learns confidential information about another
 - Data exported for research conforms to privacy promises to students, instructors

History of Stanford Online

- Stanford Center for Professional Development
- Stanford Engineering Everywhere (SEE)
- EPGY and Online High School
- iTunes U
- Stanford YouTube

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

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

f Recommend

Twitter 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

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

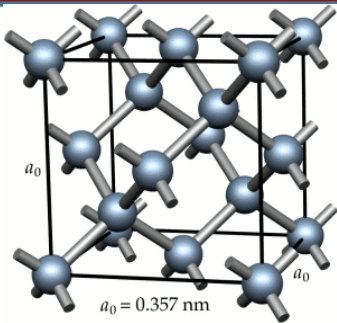
**EE282:** Computer Systems Architecture (Spring 2012)
MW 11:00am - 12:15am in Gates Hall B01 with Sue George, Christos Kozyrakis, Jacob Barton Leverich, Matthew Murray

Join

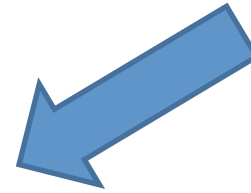
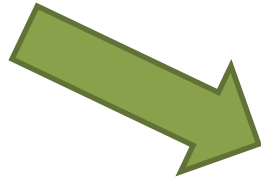
**ICS121V:** Social Media Toolkit (Spring 2012)
Th 9:00am - 10:00am in Online with Burt Lum

Join

CourseWare design goals (2009)



Reliability

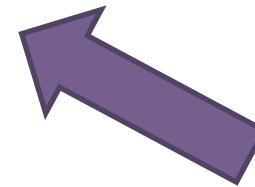
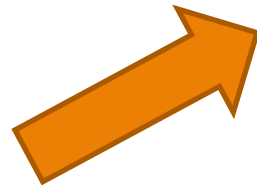


Usability

<https://courseware.stanford.edu>



Security



Performance

Initial functions (2009)

Student Interaction

- Discussion (question tracking, user ranking)
- FAQ (question ranking)
- Messaging

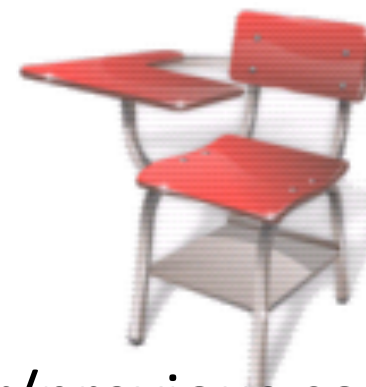


Course Management

- Lectures
- Assignments with submission & grading
- Announcements
- Calendar

Full customization

- Dashboard
- Public page (fine grained access control)
- Course Wizard (data import from Registrar/previous course)





Security design

- Access Control designed for course management
- Grades and assignments
 - Multiparty encryption (AES 256-bit)
 - Data Signing using lightweight PKI based on Webauth
 - On-the-fly decryption (data never stored in clear)
- Web security
 - Encrypted communication (SSL/HTTPS)
 - XSS/CSRF/SQL Injection Defense



Fine-grained access control

The screenshot displays the COURSEWARE interface for course CS295. The top navigation bar includes the COURSEWARE logo, user information (jhchen7), a search bar, and links for Settings, Administration, and Log out. Below this is a secondary navigation bar with tabs for Dashboard, Courses, Grades, Calendar, and Notifications (0).

The main content area is titled "CS295" and features a left-hand sidebar with navigation links: ADMINISTRATION (with sub-links for FAQ, Assignments, Course info, Access control, Lectures, and Sections), GENERAL, and MATERIALS. The "Access control" link is highlighted in red.

The "Manage Privileges" tab is selected, showing the following configuration:

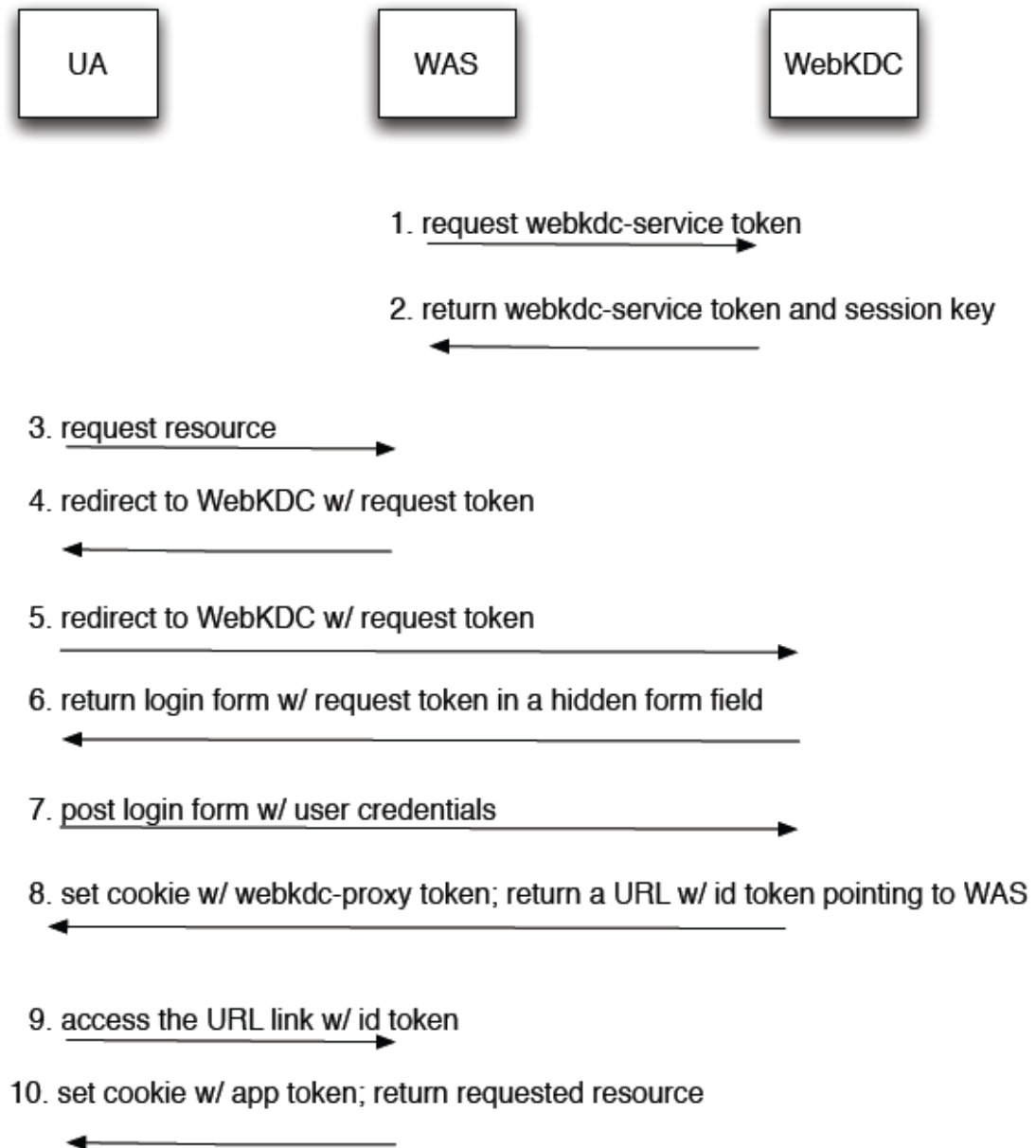
- Select a Role:** A dropdown menu is set to "Course Administrator". Below it is a checkbox labeled "Course staff?" which is currently unchecked.
- Current Privileges:** A list of permissions assigned to the selected role, including: Edit Assignments, Edit Calendar, Edit Course, Edit Grades, Forum Moderator, Manage Access Panel, Manage Members, and View Assignments.
- All Privileges:** A list of all available permissions for this role, including: Edit Assignments, Edit Calendar, Edit Course, Edit Grades, Forum Moderator, Manage Access Panel, Manage Members, Submit Assignments, View Assignments, and View Personal Grades.

Red arrow buttons are positioned between the "Current Privileges" and "All Privileges" lists to facilitate adding or removing permissions. A red "Save" button is located at the bottom right of the interface.

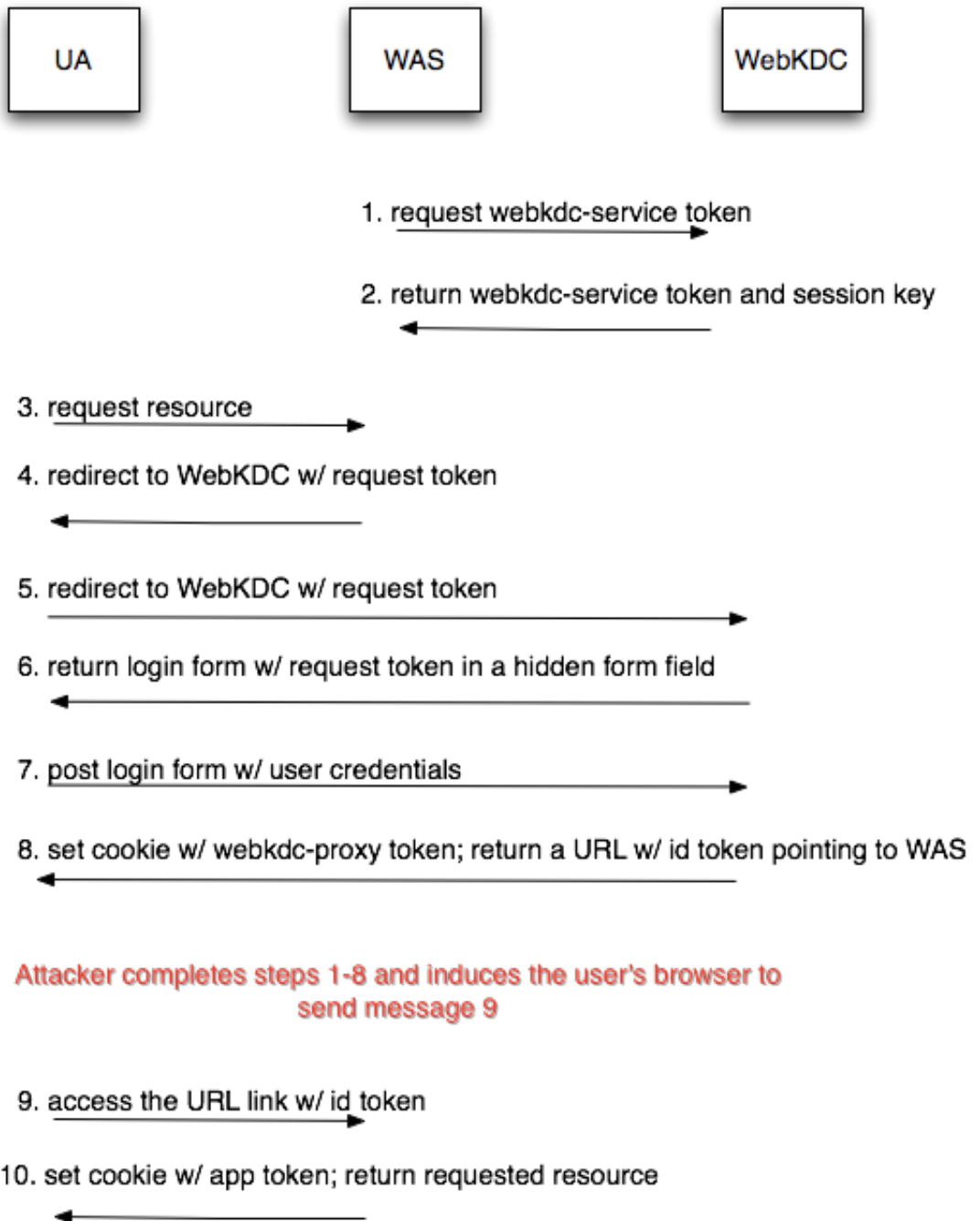
University system: WebAuth

- 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



WebAuth exploit

- Attack
 - An insider can share privileged web resources with unprivileged users without sharing login credentials
 - Attacker can steal sensitive user information by logging users into attacker's account

WebAuth - countermeasure

- Countermeasure
 - Store a nonce in a host cookie to bind messages 3 and 9, and splice in messages in between by including the nonce in the request and id tokens.
 - Verified the fix up to a finite size in our model

Looking Forward

How can new software systems support new learning models and provide data analysis needed to improve and validate them?

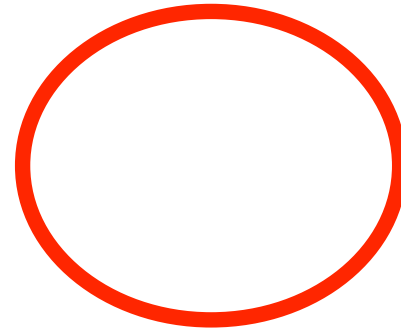
Specific concepts

- User annotation of learning material
- Reputation in group projects, peer evaluation
- Engagement and gamification
- Topic-specific algorithms and applications
 - Simulated physical environment
 - Simulated economy
 - Virtual-reality
- Assessment and stand-alone credentials
- Data analysis to
 - Evaluate learning model, content
 - Evaluate and adaptively respond to learner strengths, needs

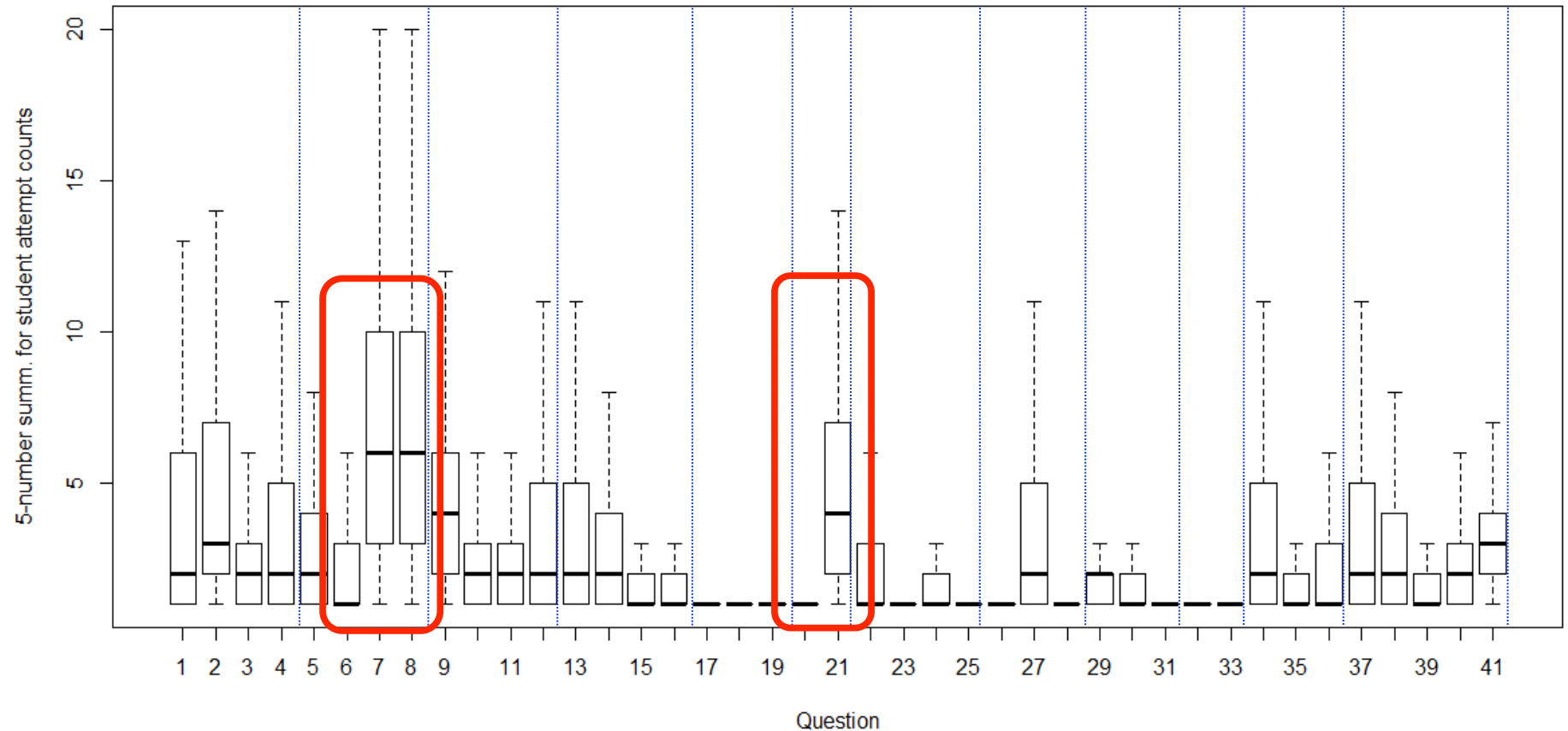
Simple Visualization of Seek Data



The image cannot be displayed. Your computer may not have enough memory to open the image, or the image may have been corrupted. Restart your computer, and then open the file again. If the red x still appears, you may have to delete the image and then insert it again.



Question Attempts



Interpreting Signals of Difficulty or Disengagement

Question taking too many attempts

Question design problem

- Strong distractors
- High complexity
- Unclear phrasing of the header or choices

Discourse problem

- Explanation was unclear
- Explanation was too difficult
- Explanation was ambiguous
- Misconception

Prerequisite problem

- Wrong assumption about pre-existing knowledge
- Very high mastery requirement of a background skill

Signals of Difficulty or Disengagement

Question taking too many attempts

```
graph TD; A[Question taking too many attempts] --> B[Question design problem]; A --> C[Discourse problem]; A --> D[Prerequisite problem]; B --> B1[•Strong distractors]; B --> B2[•High complexity]; B --> B3[•Unclear phrasing of the header or choices]; C --> C1[•Explanation was unclear]; C --> C2[•Explanation was too difficult]; C --> C3[•Explanation was ambiguous]; C --> C4[•Misconception]; D --> D1[•Wrong assumption about pre-existing knowledge]; D --> D2[•Very high mastery requirement of a background skill];
```

Question design problem

- Strong distractors
- High complexity
- Unclear phrasing of the header or choices

Discourse problem

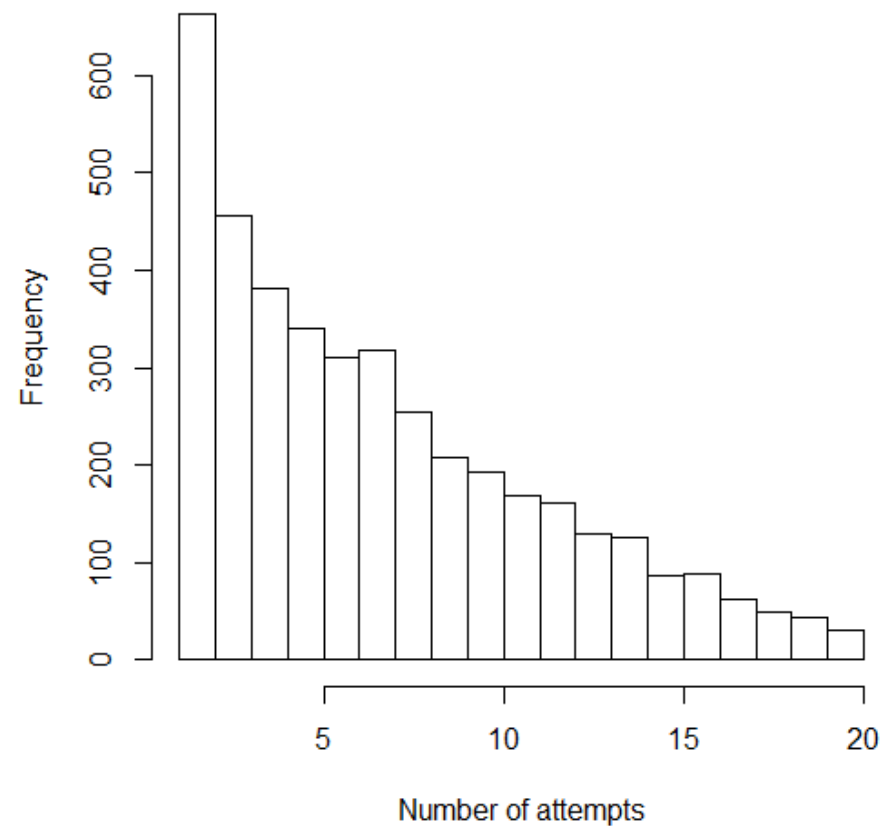
- Explanation was unclear
- Explanation was too difficult
- Explanation was ambiguous
- Misconception

Prerequisite problem

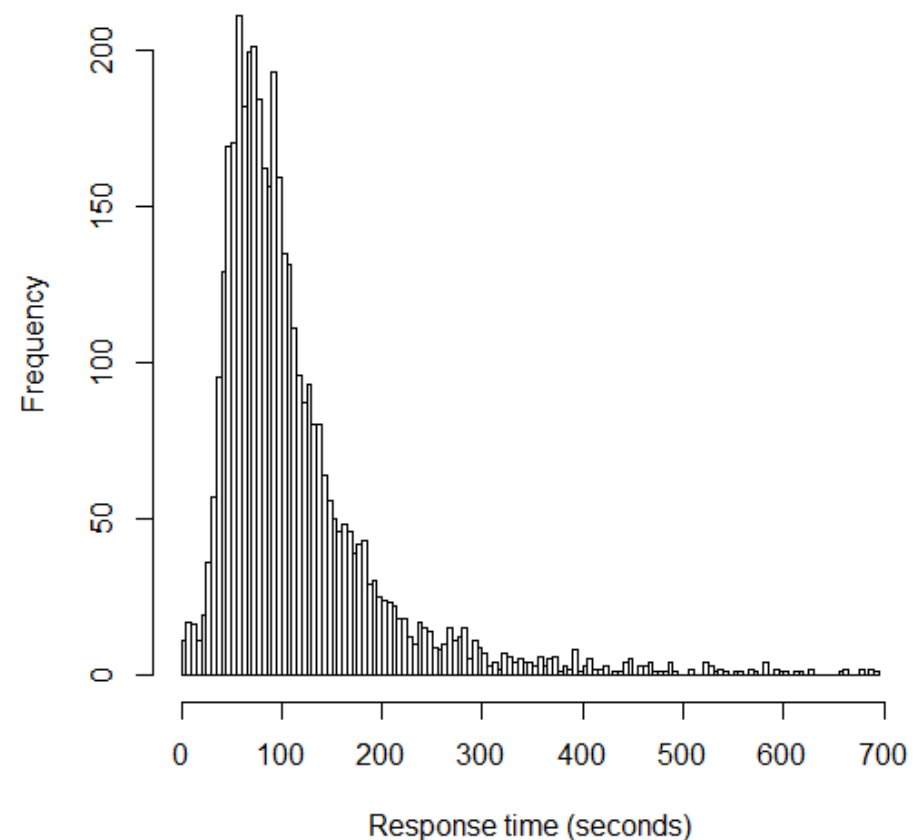
- Wrong assumption about pre-existing knowledge
- Very high mastery requirement of a background skill

Simple Assessment Analytics

Student attempt count histogram for question 7

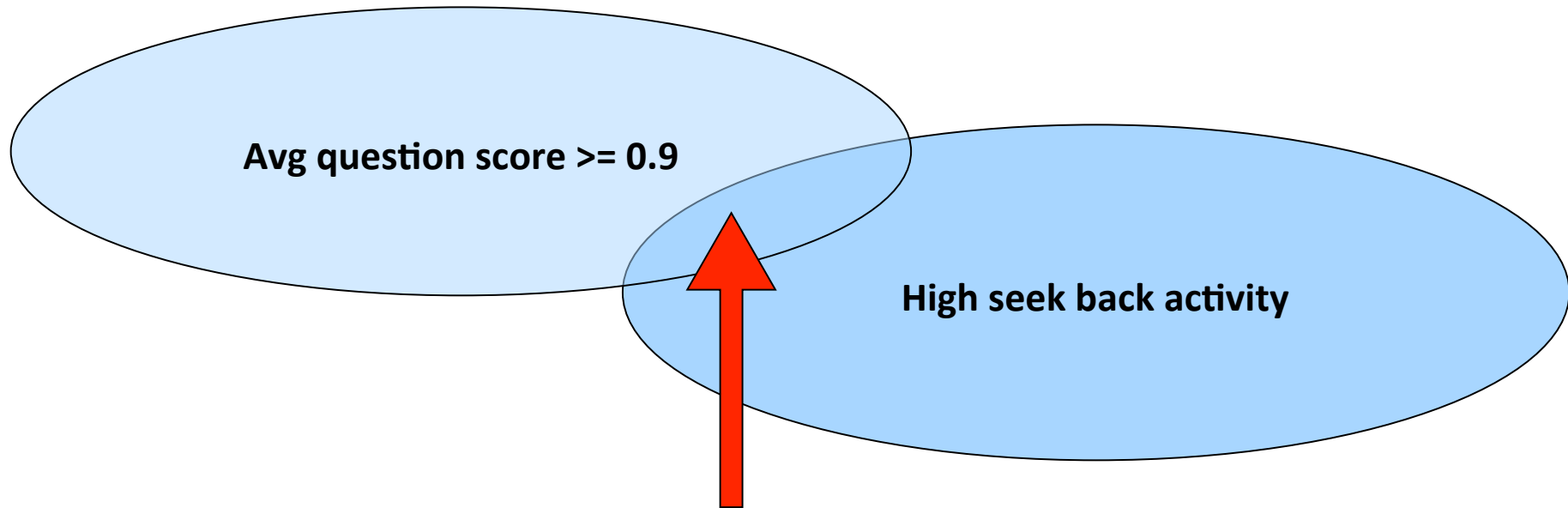


Student response time histogram for question 7



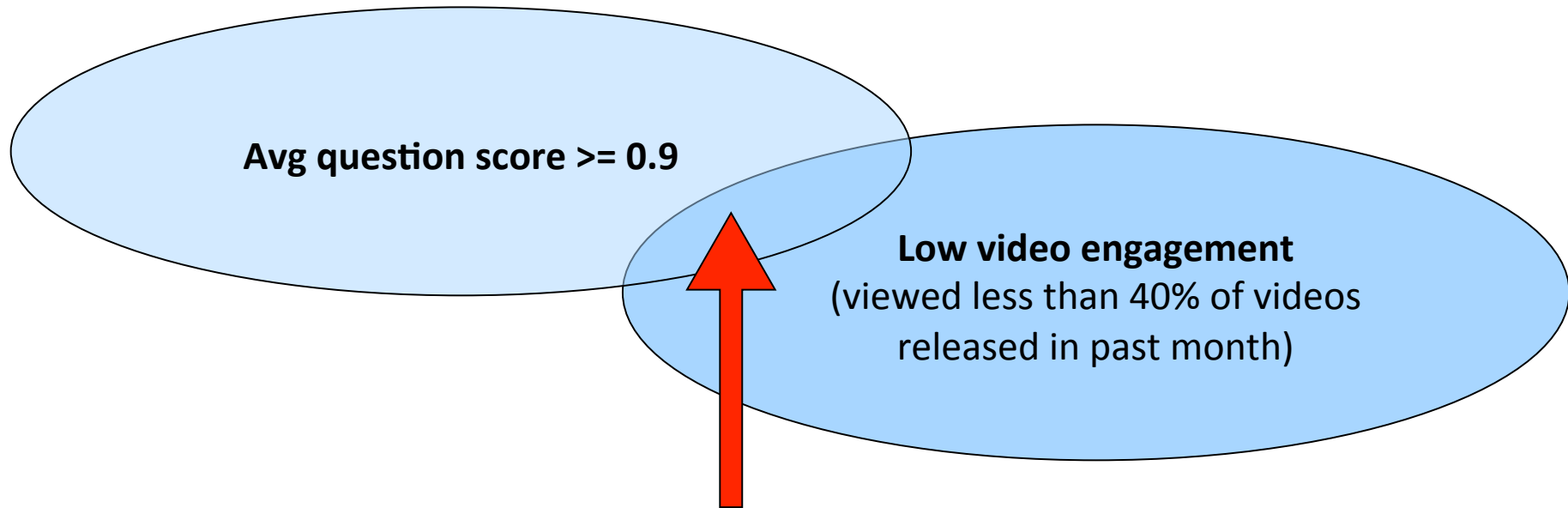
Classification of Students

Interesting Intersections

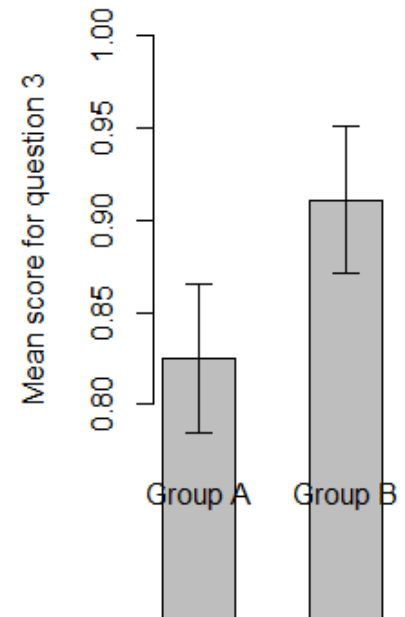
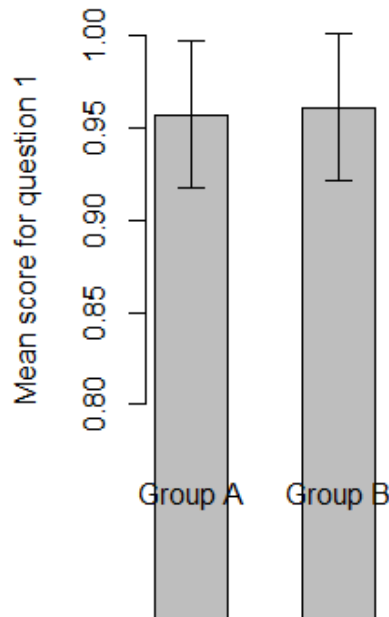
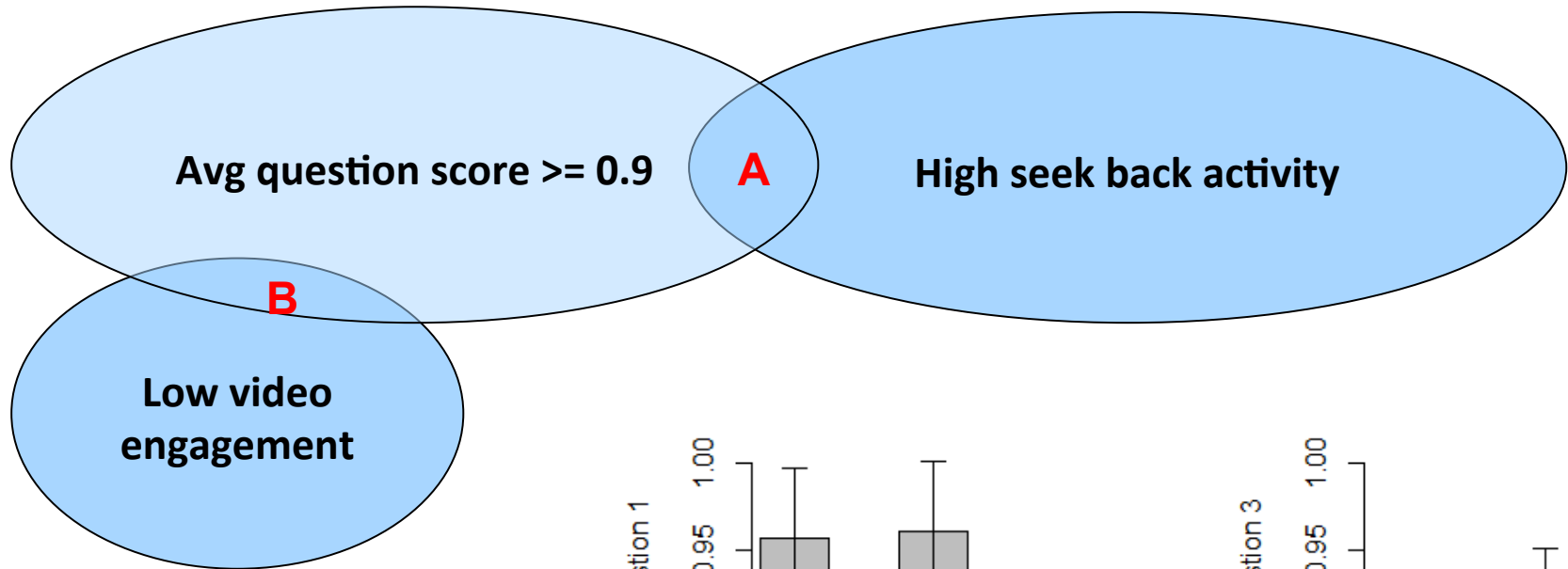


Classification of Students

Interesting Intersections



Comparison of student groups



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

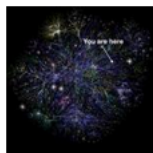
FEATURED COURSES



Election 2012

Starting: Oct 1 2012

This course focuses on the November 2012 U.S. election, and what it means for us, the state of California, the U.S.A., and the globe.



An Introduction to Computer Networks

Starting: Oct 12 2012

This is an introductory course on computer networking, specifically the Internet. It focuses on explaining how the Internet works...



Solar Cells, Fuels Cells, and Batteries

Starting: Oct 8 2012

This course focuses on the operating principles and applications of emerging technological solutions to the energy demands of the world.



A Crash Course on Creativity

Starting: Oct 17 2012

This crash course is designed to explore several factors that stimulate and inhibit creativity in individuals, teams, and organizations.

MORE COURSES

STANFORD ONLINE LEARNING PROGRAMS



Stanford on iTunes U

Over 3,000 Stanford audio and video programs are available on Apple's popular iTunes platform, including course lectures, faculty presentations and campus events.



Stanford Center for Professional Development

Qualified individuals may earn Stanford credit by completing online engineering and related courses leading to a



Stanford on YouTube

The Stanford Channel on YouTube is an archive of videos from schools, departments, and programs across the university highlighting faculty lectures and research highlights.



Stanford eCorner

Stanford's Entrepreneurship corner offers 2,000 free videos and podcasts featuring entrepreneurship and innovation thought leaders.

RECENT NEWS

Stanford School of Education course tackles challenges of digital learning

5 days 23 hours ago

Australian university joins Stanford's open-source online platform

2 weeks 3 days ago

Faculty Senate grapples with the possibilities and challenges of online learning

3 weeks 3 days ago

[READ ALL NEWS](#)

UPCOMING EVENTS

There are no events scheduled.

STAY CONNECTED

[Follow @StanfordUOnline](#)

[Stanford Online News](#)

