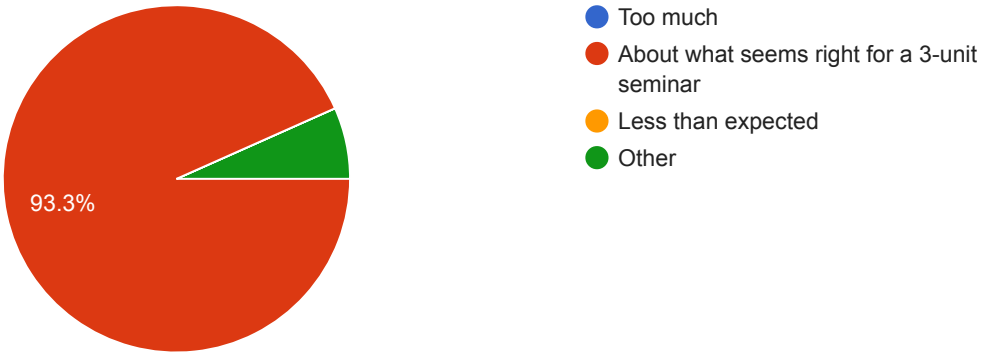
15 responses

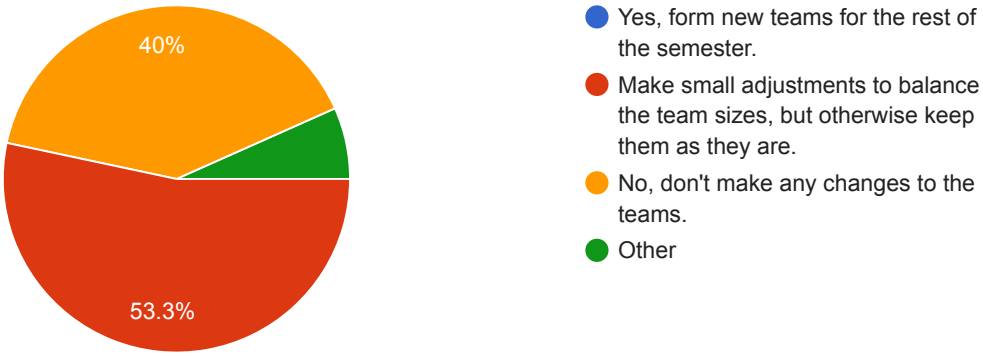
SUMMARY | INDIVIDUAL

Accepting responses

How is the workload for this class? (15 responses)



Should we change the (presenting) teams? (15 responses)



What should Dave do to make the course meetings more worthwhile?

(12 responses)

Stories!

You're already doing a good job

Instead of having presentation after presentation on different research papers, we should have a lecture style class maybe every couple weeks, where Dave could go over some fundamental cryptography things and have small

coding projects to do in class to get a better grasp on what the coding aspect of these high level TLS and other descriptions are. I know some teams tried to have the class implement a couple things, but I don't know how well that worked out. Honestly, I don't think I, personally, understood enough from the presentation to complete the task.

So far so good. More talks on recent security news could be helpful.

Plan for a little bit of time at the end of class for teams to meet and discuss next week's meeting.

Perhaps give more of a "big picture" direction for the class.

Set aside 30 minutes to cover a secondary topic himself.

Guest speakers/Skype perhaps? If we know anyone working on specific TLS projects/implementations (ex: I believe there is a contact at Google working with TLS UI notifications)

Consider doing a short presentation segment of his own in a few of the remaining classes

Thus far we've been able to find a coherent theme for each week but I think we're nearing the end of that streak. We may soon begin recycling material or talking about only tangentially related security topics. I think it would be productive to have some "starter" ideas to guide our themes in the second half of the course.

I wouldn't be upset if Dave interjected his perspective more often.

Keep the interjections during presentations coming! The perspective and knowledge is appreciated.

What should your team do to make future course meetings more worthwhile?

(14 responses)

Stick to a common story line and keep reminding the audience of the storyline throughout the seminar. Also, summarize 'What we have learned' at the end of the class.

More crypto

Start working on the presentation/blog much earlier.

I think that we should all get assigned topics before hand (by Dave or a full class brainstorm) and find research papers to present about those topics. Sometimes topics are very similar and it is good to get a wide grasp of the material. The team should also maybe focus on maybe one or two papers and do a more intensive demo or coding project with it.

Maybe adding more interactive contents.

Try to get things completed earlier.

Provide more concrete takeaways from each paper/topic.

Attempt to improve presentation cohesiveness and give knowledge beyond just what is in the papers (including background knowledge, ties to current events, etc)

Start working earlier in project cycles.

Explore topics that may be relevant to project ideas

Plan presentations earlier, practice more

My team could do a better job working "across topics." When we divvy up work for our lectures, we each stovepipe a specific topic. I believe we'd all learn more if we work together to understand all the subtopics. This would make preparation a little more involving, but it would be for the better.

We had good success discussing more high level topics, tying in the papers as context. More of that would good.

Be more proactive and quit procrastinating - our presentations would be improved by working further ahead of time.

What should other teams do to make future class meetings more worthwhile?

(13 responses)

Keep the audience actively engaged and also summarize on the 'Lessons Learned'

More Exercises

More activities!

Other teams could do a quiz thing like Kahoot. Also, in general, maybe do classes where the focus isn't research papers but a general skill or a full class on implementing TLS. That might be more interesting than just reading a research paper and talking about the topics presented in it.

So far so good.

I do not know.

Provide more concrete takeaways from each paper/topic.

Get more involved in activities.

More engaging presentations throughout the entire 2.5-hour period

Continue showing us interesting content

(We are guilty of this too.) In meetings, I think it's mostly unnecessary to trudge through slides of formulae and mathematical expressions. From my point of view, lecture should be about conveying significance, implications, and potential solutions for problems, not the nitty gritty technical specifications (unless this is essential to understanding the problem, of course, in which case an abbreviated explanation would probably suffice).

I greatly appreciate interactive demos. More would be nice.

This goes for all teams, my own included - would love to see more deliberate discussions. The lead team could compile some thoughtful questions about their topic to spark discussion, motivating the other teams to read more carefully and get engaged.

Are you sick of bagels? (15 responses)

Any other thoughts or requests? (5 responses)

I originally preferred to mix the teams up, but I did put a lot of work into managing the teams the rst half of the semester, and in a new team, I'm not sure whether I'd come off as "lazy" if I don't do much. During the second half of the semester, I'd like to focus on project/research.

As discussed above, I think that the research papers every week is getting kind of repetitive. We should have classes (either led by Dave or teams) that focus on maybe coding projects or implementing things. Somewhat like a more lecture-style class, but all of the work is done during that class period rather than pushing it off til later. I think that doing this maybe every 2 weeks would be a good break from the cycle of reading and presenting research papers. For instance, the Coq demo was a good break (even though, it was kind of part of a paper, but not really. Instead of 10 mins, maybe spend a whole class on it?). Other than that, I think the seminar is working out pretty well.

No.

None

This course had a considerable learning curve at the beginning, since I did not have background in crypto. I feel much more comfortable with the material now. For future seminars, it may be helpful to have a longer introduction/background to the material