Syllabus

cs6501: Understanding and Securing TLS

University of Virginia, Spring 2017

Meetings: Fridays, 9:30AM - noon, Thornton Hall D115

Course Objective. SSL/TLS is the world's most important cryptographic protocol, used for every secure web connection and many other purposes. Every month it seems we hear about another new major vulnerability in TLS. In this project-focused seminar, we'll take a deep dive into understanding how TLS came to be the mess it is today, look into some of the vulnerabilities in detail, and study methods for making TLS more secure. We will work as a group to contribute to open source projects to improve the security of TLS.

Expected Background: Students are expected to enter the class with introductory background in cryptography (sufficient to understand symmetric and asymmetric cryptosystems, cryptographic hash functions, and digital signatures) and experience in systems programming (comparable to a good undergraduate operating systems course). If you do not have this background, you are still welcome to take the course, but will need to do some work on your own to be prepared before the semester begins (see the course site for links to recommended preparation materials).

Coordinators:
Hussain Almohri (visiting from Kuwait University)
David Evans (evans@virginia.edu). My office is Rice 507.

Course Expectations

Students in the seminar are expected to:

– Lead discussions on interesting topics during the class meetings. For each week, there will be two groups of two students charged with preparing a topic and leading the discussion.

– Particpate actively in class meetings. This means being prepared to contribute by doing the assigned preparation (which will typically involve reading a few research papers, but may involve other things also) and thinking about the materials deeply to be able to contribute well to discussions.

– Produce scribe "blogs" for 2-3 topics. For each topic, there will be students assigned to write-up a blog about the topic to post on the course site. Students responsible for posting the blog summary will be different from the ones charged with leading the topic discussion, but should work closely with the leaders on the posted write-up.

– Work in a small team to conduct projects that will contribute usefully to the TLS ecosystem. Projects may contribute to open source implementations of TLS, provide resources for testing and deploying TLS, analyze the state of TLS deployments today, or adress other issues related to secure web connections.

– Work with the class to produce a systematization of knowledge paper on the security of TLS. Everyone will be expected to contribute to this, with the goal of jointly producing a publishable paper that systematizes what is currently known about TLS and the ecosystem around it.

Communications

Course Website: *https://tlseminar.github.io/*. All course materials will be posted on the course website, and students will be expected to provide materials to add to this site.

Slack: *https://tlseminar.slack.com*. We will use a slack group for class communications. You can join using any `@virginia.edu` email address. You can also create slack channels for your team communications.

Honor and Responsibility

We believe strongly in the value of a *community of trust*, and expect all of the students in this class to contribute to strenghtening and enhancing that community. The course will be better for everyone if everyone can assume everyone else is trustworthy. The course staff starts with the assumption that all students at the university deserve to be trusted.

In this course, we will be learning about and exploring some vulnerabilities that could be used to compromise vunlerable websites. **You are trusted to behave responsibility and ethically.** You may not attack any website without permission of the site owners, and may not use anything you learn in this class for evil. If you have any doubts about whether or not something you want to do is ethical and legal, you should check with the course instructor before proceeding.

Area Requirements

Note for CS Graduate Students. This course is mislisted in SIS (indeed, it is a "bug" in the setup of SIS that cannot be overcome that requires all grad courses to be assigned areas) as counting for the "Computer Systems" and "Theory" area requirements. As per the actual rules, as a cs6501 seminar the course does not a priori count for any particular areas. It may be possible to count it for any area, but it would be up to you to make the case to your committee that it should count for a given area. In most cases, this will depend a lot on what you individually do in the class - for example, you could select presentation topics and a topic for you project that would make a strong case for counting it for the "Theory" area, but someone else who does a systems-focused project would be able to count it for a different area. I can help provide guidance on this, but it is ultimately up to your committee to decide if a course counts for a particular area requirement.

