Data Communication and Networks	**Course Syllabus**
CSCI-759 Fall 2018	**January 23, 2019**

Location	Golisano Hall (GOL)-3435
Time	Tuesday and Thursday 8:00AM–09:15AM
Forum	`https://mycourses.rit.edu/d2l/home/739080`
Instructor	Prof. Taejoong (Tijay) Chung
Contact	`tjc@cs.rit.edu` (put "[CSCI-759]" in the subject line)
Office hours	Tuesday, 9:15PM–10:30PM, GOL-3525

DESCRIPTION (from the Registrar)

This course examines current topics in Systems. This is intended to allow faculty to pilot potential new graduate offerings. Specific course details (such as prerequisites, course topics, format, learning outcomes, assessment methods, and resource needs) will be determined by the faculty member(s) who propose a specific topics course in this area. Specific course instances will be identified as belonging to the Distributed Systems cluster, the Architecture and Operating Systems cluster, the Security cluster, or some combination of these three clusters.

DESCRIPTION (from me)

A public key infrastructure (PKI) provides secure communications between two different entities over an untrusted network. Due to this ability, PKIs are now central to security on the Internet: there are a number of large-scale PKIs in use today such as DNSSEC, HTTPS, and the RPKI. This course examines basic network security models and public key infrastructure that entwines multiple layers of the network stack: application, transport, and network layer. Topics include concepts in basic threat models in networking, public key infrastructure, data-driven approach for securing Internet, etc. Students are required to write critiques on assigned papers, propose and complete a research project individually or in teams, write a research manuscript, and give presentations on a related topic. This course instance belongs to the Distributed Systems cluster and Security cluster.

LOGISTICS

The class will twice per week, online and offline combined class, for 75-minute sessions. The course will be mostly based on research papers. Each student is expected to present a research paper throughout the semester and all students are requred to read the paper before the class and actively participate the in-class discussion. Students are also required to pick the research topic related to the class, and perform their own research project.

TEXTBOOK

The recommended (but not required) textbooks for the course is

Peter Gutmann. *Engineering Security* (https://www.cs.auckland.ac.nz/ pgut001/pubs/book.pdf)

Johannes A. Buchmann, Evangelos Karatsiolis, Alexander Wiesmaier. *Introduction to Public Key Infrastructures*

ONLINE DISCUSSION

To encourage more in-depth discussion beyond the class, students need to discuss the pros and cons of the paper discussed at the offline class. Every week, there are 7 students (3 students for the pros, 3 students for the cons of the paper, and the other student for organizing and summarizing the discussion) are assigned to discuss two papers. The deadline of the discussion is at the end of date of the online class (e.g, 11:59:59pm on Thursday); please find the schedule on the course webpage regularly. To give enough time for organizers to summarize the discussion by the deadline, it is *strongly* encouraged for the other students to finish their discussion by the noon.

The below is an example of the discussion for the paper [DNSSEC 01]:

Reviewer A:

> This is a very well written measurement study that reveals the difficult path towards widespread DNSSEC adoption.
>
> The paper starts with a good introduction to DNSSEC that is at the same time sufficiently high-level to be understood by readers who are familiar with DNS but not with its security extensions, and sufficiently detailed to allow the reader to follow the more technical measurements presented in the paper.
>
> The paper also does a good job at summarizing previous work in this area, and to differentiate the methods and findings of this paper compared to related results presented by others. However, I did not see the SecSpider project (secspider.verisignlabs.com) mentioned or in the references.
>
> Not surprisingly, DNSSEC deployment for second-level domains is still tiny (around 1%). This is in line with previous findings. What is somewhat surprising, is that the deployment for the top 10K Alexa sites is also very small, and that a large fraction of these DNSSEC-enabled domains publish keys that cannot be validated.
>
> On the server side, the daily and hourly scan approach seem a very reasonable trade off between detailed information gathering and scalability of the solution. One question I had is why the scans are limited to checking only the SOA, DNSKEY, and related signatures. I wonder if it would be useful to also check A records for <domain> or www.<domain>.
>
> I'm also wondering if the finding about "Domain Monster, bulk-signing over 37,000 new domains without placing the proper DS records" is due to IT people forgetting to communicate the DS records to the TLDs, or if some blame should be put on the TLDs themselves, perhaps because they don't provide an automated/convenient way to do bulk updates of DS records?
>
> The resolver-side measurements are the most interesting, in my view. I particularly like the way the authors leveraged the Luminati network to perform large-scale measurements on a very diverse set of resolvers.
>
> The results are very interesting, and show that even large ISPs and DNS operators (e.g., Level3 and Dyn) seem to have a hard time correctly managing DNSSEC operations.
>
> It is also surprising (and somewhat concerning) to find that even the BIND developers may have misinterpreted the RFCs, when it comes to sining both the KSK and ZSK.

EXAMS

There will be no exams for this class.

GRADING

The breakdown of the grades in this course is

35%	Paper presentation
20%	Paper discussions
20%	Research Project
25%	Participation

paper lists (can be added more)

1. Censys: A Search Engine Backed by Internet-Wide Scanning [CCS15]
2. An End-to-End Measurement of Certificate Revocation in the Web's PKI [IMC15]
3. Measuring and Applying Invalid SSL Certificates: The Silent Majority [IMC16]
4. Measurement and Analysis of Private Key Sharing in the HTTPS Ecosystem [CCS16]
5. Analysis of SSL certificate reissues and revocations in the wake of Heartbleed [IMC14]
6. Tracking Certificate Misissuance in the Wild [Oakland18]
7. The Security Impact of HTTPS Interception [NDSS17]
8. The Rise of Certificate Transparency and Its Implications on the Internet Ecosystem [IMC18]
9. A First Look at Certification Authority Authorization (CAA) [CCR18]
10. Does Certificate Transparency Break the Web? Measuring Adoption and Error Rate [Oakland19]
11. Is the Web Ready for OCSP Must Staple? [IMC18]
12. Mission Accomplished? HTTPS Security after DigiNotar [IMC17]
13. CRLite: a Scalable System for Pushing all TLS Revocations to All Browsers [Oakland17]
14. A Longitudinal, End-to-End View of the DNSSEC Ecosystem [Security17]
15. Understanding the Role of Registrars in DNSSEC Deployment [IMC17]
16. DNSSEC and Its Potential for DDoS Attacks [IMC14]
17. Security by Any Other Name: On the Effectiveness of Provider Based Email Security [CCS15]
18. RFC7671 (https://tools.ietf.org/html/rfc7671)
19. Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security [IMC15]
20. Measuring DANE TLSA Deployment [TMA15]
21. Why Is It Taking So Long to Secure Internet Routing [ACMQueue14]

22. RFC6480 (https://tools.ietf.org/html/rfc6480)
23. On the Risk of Misbehaving RPKI Authorities [Hotnets16]
24. MaxLength Considered Harmful to the RPKI [CoNEXT17]