Public Key Infrastructure and Network Security	**Course Syllabus**
CS 6204 Fall 2020	**June 17, 2020**

Location	Online Class
Time	Mondays and Wednesdays 05:30PM–06:45PM
Forum	TBD
Instructor	Prof. Taejoong (Tijay) Chung
Contact	tijay@vt.edu (put "[CS 6204]" in the subject line)
Office hours	TBD

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 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*

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. Roll, Roll, Roll your Root: A Comprehensive Analysis of the First Ever DNSSEC Root KSK Rollover[IMC19]
18. Security by Any Other Name: On the Effectiveness of Provider Based Email Security [CCS15]
19. You Are Who You Appear to Be: A Longitudinal Study of Domain Impersonation in TLS Certificates [CCS19]
20. RFC7671 (https://tools.ietf.org/html/rfc7671)

21. Neither Snow Nor Rain Nor MITM... An Empirical Analysis of Email Delivery Security [IMC15]

22. Measuring DANE TLSA Deployment [TMA15]

23. Why Is It Taking So Long to Secure Internet Routing [ACMQueue14]

24. RFC6480 (https://tools.ietf.org/html/rfc6480)

25. On the Risk of Misbehaving RPKI Authorities [Hotnets16]

26. MaxLength Considered Harmful to the RPKI [CoNEXT17]

27. RPKI is Coming of Age: A Longitudinal Study of RPKI Deployment and Invalid Route Origins [IMC19]