CSCI S-49a

Cryptography and Identity Management for Blockchain and Cloud Applications

Summer II (3 Weeks) - 2019

Class Meeting Times:

Course start and end dates: July 15, 2019 to August 2, 2019

Monday – Thursday (6:30 PM – 9:30 PM EST), Science Center Room #110

Online Q&A sections: Saturdays 10:00 AM EST (via Zoom Conferencing)

Class Objectives:

Confidentiality, integrity, availability, authentication, authorization and accountability are the most critical security requirements that serves as the basis for deploying and delivering trustworthy IT applications, and services in enterprises, mobile devices and via Cloud providers. Adopting cryptography and identity management techniques addresses those security requirements, and has become the vital part of all business applications and electronic transactions. **This course provides the ground-up coverage on the high-level concepts, applied mechanisms, architecture and real-world implementation practices of using cryptography and identity management techniques applied to Blockchain and Cloud hosted applications and services.**

To begin with, the course will examine the fundamentals of cryptography, access control principles, identity management and assurance strategies applied to IT applications and Cloud infrastructure based services. The course will delve deep in to the use of cryptographic algorithms, mechanisms and applied technologies intended for encrypting data in transit, use, and at rest, managing cryptographic key operations lifecycle, private blockchain infrastructures (Ethereum/Hyperledger Fabric), integrating public-key infrastructures and certificate authorities, verifying and validating personal, device and host identities with digital signatures, creating directory services, enabling single sign-on authentication, enforcing access control and authorization policies in IT resources, monitoring, logging and recording audit trails and leading to meet compliance with industry and regulatory mandates. The course will describe Blockchain infrastructures, industry standard based services/protocols such as TLS, IPSec/IKE, LDAP, OCSP, SAML, XACML Oauth2, Open ID, and leverage data protection and identity management guidelines set forth by NIST, ENISA and Cloud Security Alliance (CSA).

Students will learn and develop understanding of the following:

- Fundamentals of cryptography and its usage scenarios.
- Understand the concepts, guiding principles, applied cryptographic mechanisms used in Blockchain and Cloud infrastructures.
- Design security architectures that assures comprehensive data protection using encryption at all layers of IT infrastructure, enforces end-to-end identity and access management controls, monitoring and auditing processes and compliance with industry and regulatory mandates.
- Use of Cloud based services and technologies solutions that builds on Public-Key infrastructures (PKI), Cryptographic Key Management Services (KMS), Certificate Authorities (CA), Cryptographic Hardware Security Modules (HSM), Identity and Access Management (IAM) infrastructures for directory services, identity provisioning, Zero Knowledge Identity, Web Single Sign-on (SSO), Multi-factor Authentication (MFA) and enabling identity federation across enterprises and Cloud providers.
- Hands-on experience with cryptographic libraries and providers (ex. OpenSSL. JCE) and identity Management solutions (ex. Shibboleth, OpenLDAP, Active Directory, OpenSAML, OAuth2, Google Authentication, OpenID Connect) using a Cloud provider infrastructure.
- Understand emerging Quantum resistant cryptographic methods like Post-Quantum Cryptography (PQC) algorithms and Quantum Key Distribution (QKD)
- Understanding of Security testing and benchmarking for Identity and Access Control policies.
- Understand the industry security standards (ex. NIST 800-53), regulatory mandates (ex. GDPR), audit policies and compliance requirements for data protection and privacy in Cloud hosted applications and services.

Class Meeting Times:

This course will be offered via both on-campus and online distance learning.

Sections will be delivered via Zoom conferencing during weekends of the 3-week course (Saturdays 10:00 AM)

Class Prerequisites:

CSCI E-49 or CSCI E-90 or CSCI E-118 any equivalent. Alternatively, hands-on experience with web application development and/or systems administration using a Cloud provider will be helpful. No programming experience required.

Materials of Instruction:

Class Notes

- This class covers a great deal of information about Cryptography and Identity Management standards and technologies, so no single textbook can cover it all. Class notes will be provided for all topics covered.
- Guidelines and best practices prescribed by NIST, Cloud Security Alliance and ENISA.
- Instructor will provide weekly presentation slides, hands-on demonstration and cookbooks for Cloud based exercises (using AWS).

Recommended Texts

- Network Security Essentials (6th , William Stallings, Pearson Education
- RSA's Official Guide to Cryptography, Steve Burnett et all (RSA Press)

Weekly Topics

Week 1 July 15 – July 18 (12 hours)	Cryptography basics: Symmetric/Asymmetric and Hashing algorithms
	Digital Signatures, Public-key Infrastructure (PKI) and Digital Certificates
	Key management lifecycle and policies
Week 2 July 22 – July 25 (12 hours)	Applications: Transport layer Security using Public-key Infrastructure
	Applications: Deploying Blockchain with Ethereum/Hyperledger
	Applications: Data Encryption and Key Management in Cloud
Week 3 July 29 – Aug 1 (12 hours)	Identity and Access Management, Directory Services and Provisioning
	Web Single Sign-On (SSO), Federation and Web Identity Tokens
	Applications: Identity Management and Data Protection in Cloud

Course Grading Criteria:

Percent	Component
50%	3 Assignments (Open response and Lab work)
50%	3 Quizzes (Online)

Grading Policy:

https://www.extension.harvard.edu/resources-policies/exams-grades-transcripts/grades

Course Participation:

- Summer school policy requires attendance in all classes.
- Review the lecture topics (All lectures and sections will be recorded and available online)
- Attend online sections (during weekends) for Q&A, assignment reviews, labs demo, and project help.
- Assignments (open response & labs) will be posted every week. Complete & submit them before its due date
- Prepare for Weekly online quizzes
- All practical exercises must use Harvard provided Cloud account.
- All assignments must be student's original work, with sources properly cited.
- All assignment/work submissions must be made in Microsoft DOC or Adobe PDF formats.
- Students are expected to spend atleast 15 – 20 hours per week (during the 3-week course) for reviewing course work and completing assignments.

Class work and Lab exercises

- For all lab and practical purposes, this course will use "Amazon Web Services (AWS) Cloud Provider" environment. Students are required to register and obtain **AWS Educate (Free-tier) account** using their Harvard email account (ex. youremailid@g.harvard.edu). If the student already has an account with AWS Educate using Harvard email-id, no action is necessary.
- For more information, refer to https://www.awseducate.com
- **IMPORTANT**: If you are registered for CSCI S-49a, you may contact softwarerequest@labstaff.dce.harvard.edu before the course begins and obtain your AWS credit.

- All students must have access to a notebook computer with Wi-Fi running Microsoft Windows, Mac OS X, or Linux (Ubuntu, SuSE, or Red Hat). For Microsoft Windows users: Administrator access to the computer is required. Students should familiarize with using Secure Shell (SSH) to access the Cloud environment using SSH clients (ex. Putty) -- Guidance will be provided for those need help.

Requirements for Graduate and Undergraduate credit students

- Both graduate and undergraduate credit students are expected to meet all the course expectations completing all required Quizzes and Assignments.

Academic Integrity Requirements:

Students are responsible for understanding Harvard Summer School responsibilities, expectations and policies on academic integrity (https://www.summer.harvard.edu/student-responsibilities) and how to conduct themselves responsibly with honesty, and use sources responsibly. To know more about academic citation rules follow the Harvard guide to using sources (https://www.summer.harvard.edu/resources-policies/resources-support-academic-integrity) where students will find links to the Harvard Guide to Using Sources and two free online 15-minute tutorials to test your knowledge of academic citation policy. The tutorials are anonymous open-learning tools. Not knowing the rules, misunderstanding the rules, running out of time, submitting the wrong draft, or being overwhelmed with multiple demands are not acceptable excuses. There are no excuses for failure to uphold academic integrity.

Accessibility:

The Summer School is committed to providing an accessible academic community. The Accessibility Office offers a variety of accommodations and services to students with documented disabilities. Please visit https://www.summer.harvard.edu/resources-policies/accessibility-services for more information.

Instructor:

Ramesh Nagappan
nramesh@post.harvard.edu