RX-M - Cryptography in Cloud Native Systems

Code:	CN2-C-CNS
Length:	3 days
URL:	View Online

This in-depth hands-on course introduces developers, security professionals and other technology staff to the principles and practices driving modern cryptography. Day one begins with a cryptography overview and coverage of both block and stream ciphers. Block cipher modes for streaming systems are covered along with schemes for encryption at rest on prem and in the cloud.

Day two ties in hashing and signing technologies along with keys and key exchange. On the practical side, day two introduces attendees to certificates, PKI, TLS, IPSEC, WPA2 and various MAC and digital signature schemes used to authenticate binaries and containers. Each module in the course includes a hands-on lab, giving attendees a chance to work with common tools and technologies, providing practical insight to accompany the theory.

Day three introduces various key management schemes and tools such as Hashi Corp Vault and common cloud native platform solutions. The final modules cover authentication and encryption platforms such as Kerberos and SSH, with a deeper look at GSSAPI and other supporting technologies.

Upon completion, attendees will have the knowledge and skills necessary to create and analyze best practice driven cryptographic systems that are robust, efficient and secure.

Skills Gained

- This three day hands-on course is designed to provide developers and security professionals with a solid grounding in digital cryptography covering both theory and modern common practice in a cloud native environment.

Who Can Benefit

- Developers, Security Team Members, IT and QA Staff, Architects and Technical Managers

Prerequisites

- General technology background. Each attendee must have a laptop with internet access and the ability to run a 64 bit virtual machine to complete the lab assignments.

Course Details

Cryptography in Cloud Native Systems

- Day 1 - Ciphers and Encryption

1. Cryptography Overview

2. Block Ciphers
3. Stream Ciphers and Modes
4. At Rest Encryption

- Day 2 - Hash Functions and Key Exchange

1. Cryptographic Hashing
2. Key Exchange Schemes
3. Signing, PKI, TLS and Cipher Suites
4. IPSEC, Wireless and Wired Encryption

- Day 3 - End to End Solutions

1. Key Management
2. Kerberos
3. GSSAPI, SASL and SSH
4. Additional Topics
