Data Engineering & Security
REAL·T

Corso Executive:
IMPLEMENTAZIONE SICURA DI PRIMITIVE CRITTOGRAFICHE SIMMETRICHE
(Real-World Cryptography)

Un percorso avanzato dedicato alla progettazione, implementazione e valutazione delle primitive crittografiche simmetriche, con particolare attenzione agli errori che possono compromettere confidenzialità, integrità e autenticità dei dati.
Il corso analizza algoritmi, modalità operative e meccanismi di autenticazione, evidenziando le vulnerabilità che emergono quando primitive formalmente sicure vengono integrate in modo scorretto.

Temi principali
Cifratura simmetrica e gestione delle chiavi
Block cipher e stream cipher
Modalità operative e autenticazione dei dati
Cifratura autenticata
Nonce, initialization vector e gestione dello stato
Padding e relative vulnerabilità
Derivazione e separazione delle chiavi
Randomness e generazione sicura dei parametri
Implementazioni constant-time
Side-channel attack e vulnerabilità implementative
Validazione degli input e gestione sicura degli errori
Analisi di casi reali e failure mode
Secure coding per software crittografico

Obiettivo
Comprendere non solo come funzionano le primitive crittografiche simmetriche, ma soprattutto come selezionarle, combinarle e implementarle correttamente nei sistemi reali, evitando errori capaci di annullarne le garanzie di sicurezza.

Per professionisti della cybersecurity, software engineer, security engineer, architect e sviluppatori di sistemi ad alta criticità.

Per informazioni scrivere a:
segreteria@realt.it

Sede di svolgimento: Roma