

Quantum attack threat risk analysis

CREDEM

BANCA

Le **tecniche** e le **tattiche di attacco** stanno subendo inevitabilmente una profonda rivisitazione quando si considera la possibilità, da parte di un attaccante, di utilizzare computer quantistici con potenze di calcolo sufficienti per rompere o indebolire la crittografia tradizionale.

DIRECT-ENCRYPTION CENTRIC

Minacce provenienti dalla crittoanalisi, falsificazione (forging) dei certificati digitali X.509

Intercettazione nello scambio di chiavi crittografiche DH/ECDH

Tampering firme digitali con crittografia RSA/ECC

Indebolimento o rottura protocollo TLS con cipher-suite non quantum-resistant

Attacchi su dati a riposo con crittografia simmetrica AES indebolita mediante attacchi brute force basati su Grover

Bypass schemi di autenticazione MFA/OTP

Attacchi MITM mediante decryption TLS o sessioni VPN

HNDL

Cattura non autorizzata del traffico TLS consente esfiltrazione di dati da oggetti cloud storage (S3 buckets, Azure blobs, ecc).

Compromissione archivi con crittografia debole (es. AES 128)



INDIRECT

Encryption-protected data, credentials or channels

Falsificazione o decryption di ticket Kerberos cifrati con AES-RC4-HMAC e conseguente privilege escalation

JWT o OAuth tokens esposti firmati con RSA/ECC

MFA session hijacking

Scenari di broken authentication su servizi remoti con autenticazione basata su kerberos o certificati

Compromissione session token encryption su servizi cloud

Furto e riuso di segreti (stuffing)

Chiavi SSH o certificati esposti con chiavi di crittografia RSA/ECDSA compromesse

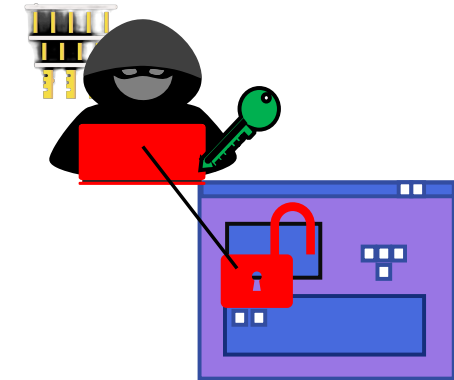
Attacchi brute force su password e password managers

Considerazioni sulla quantum threat risk analysis



La minaccia degli attacchi tramite computer quantistici riguarda la **crittografia** in tutti gli scenari di protezione dei dati nei quali viene utilizzata.

Il potenziamento generale delle misure di sicurezza è certamente utile, ma la possibilità di attacchi quantistici richiede misure preventive e contromisure specifiche.



L'impatto più rilevante della minaccia HNDL è sulla crittografia **asimmetrica** (a chiave pubblica) sulla quale si basa la sicurezza della comunicazione tra le parti. Il motivo è che in presenza di computer quantistici sufficientemente potenti **cedono i fondamenti matematici** che sono alla base dello **scambio delle chiavi** o del **riconoscimento dell'autenticità** tramite **firma digitale**.

La crittografia simmetrica diverrà presumibilmente più debole e pertanto dovrà essere aggiornata con chiavi di lunghezza adeguata.

Adozione di misure per mitigazione quantum risk

CREDEM

BANCA

Seguendo le linee guida del framework PQCC (Post Quantum Cryptography Coalition), il Gruppo CREDEM sta formando i team IT e di Cybersecurity per governare la transizione alla crittografia post-quantistica (PQC), adottando un approccio **integrato Zero Trust** e **Appsec driven** per proteggere i propri asset IT ed acquisire o integrare soluzioni **crypto-agili**.

01

Formazione su PQC

Tesi di Master ICT

Aggiornamento
formazione interna dei
team di sicurezza e del
sistema informativo

Partecipazione ad eventi e
tavole rotonde dedicate

Analisi security report

Accesso a simulazioni di
crittoanalisi

02

Organizzazione servizio SECURE

Potenziamento ed
adeguamento
dell'organizzazione delle
Funzioni del servizio
SECURE di Gruppo
(Governance e Operations)

03

Cryptography Hardening

Cryptography hardening
con approccio "Zero
Trust"

Rafforzamento linee
guida architetturali e
requisiti sulla protezione
dati

Potenziamento controlli
di sicurezza sulla
crittografia

04

Implementazione PQC

Cryptography assessment

Quantum threat modeling

Hardening dei
meccanismi di
autenticazione

Sostituzione algoritmi
vulnerabili ad attacchi
quantistici

05

Crypto-Agility

Definizione dei requisiti
per l'integrazione di
soluzioni in scenari
crittografici ibridi

Monitoring dell'efficacia
delle soluzioni attraverso
l'integrazione dei
processi di Vulnerability
Management

Cryptography Hardening nella security architecture

CREDEM

BANCA

Rafforzamento delle linee guida architetturali, delle policy di governo della crittografia e delle strategie di protezione dei dati

Adeguamento checklist Architetturali e policy di governo della sicurezza

Aggiornamento checklist
architetturali con requisiti
crittografici specifici

Aggiornamento policy in
materia di crittografia

Adeguamento strategie di protezione dati

Aggiornamento sulla
classificazione dei dati sensibili
da proteggere mediante
crittografia, in base alla data
retention

Approccio Privacy by Design
per progettare i sistemi con
algoritmi quantum-safe

Integrazione PQC - SSDLC

- Rivisitazione dei piani
di obsolescenza
hardware e software in
ottica PQC
- Rafforzamento **SSDLC**
raccomandazioni
secure coding e
pratiche DevSecOps in
ottica PQC
- Definizione criteri per
la **valutazione**
crittografica di librerie
terze parti



Aderenza agli standard Crittografici e compliance normativa

Riferimento agli standard
crittografici core (NIST, PCI
DSS)

Riferimento alla
regolamentazione UE (DORA e
NIS2)

Attuazione raccomandazioni del Framework OWASP in ottica PQC



Fonte: OWASP TOP 10 2025

Attuazione misure di contrasto a

- **Cryptographic Failures**
- **Authentication Failures**
- **Software Supply Chain Failures**



Fonte: OWASP Cheat Sheet Series Project

- Adeguamenti alla **versione 1.3 del TLS** con modalità effimera
- Rafforzamento misure preventive sulla **gestione delle chiavi**
- Rafforzamento misure di **prevenzione** dagli **attacchi JWT**
- Rafforzamento della **protezione** e della gestione dei **segreti**

Potenziamento metodologia di test ASVS-based

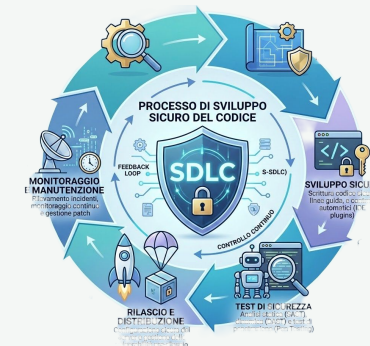
Fonte: OWASP ASVS (Application Security Verification Standard)



- **Cryptography**
- **Secure Communication**
- **Data Protection Cryptography verification** per la sicurezza della **Supply Chain**

Rafforzamento controlli SSDLC in ottica PQC

- Aggiornamento **checklist di verifica applicativa** su algoritmi **crittografici** utilizzati
- Potenziamento ed automazione delle **verifiche crittografiche nei test di sicurezza** (SAST/DAST, Vulnerability scan, pentesting)
- Estensione controlli verso terze parti



Cryptography Assessment

1

- **Scope dell'analisi:** rete esterna, rete interna, asset IT, codice e database
- **Strumenti dedicati:** adozione di strumenti specifici per la crypto discovery e la simulazione avanzata
- **Cryptography discovery:** detection di protocolli ed algoritmi crittografici vulnerabili
- Analisi della **Cryptography Bill Of Materials (CBOM)**



Quantum Threat Modeling

2

- **Applicativo:** modellazione specifica dei rischi quantistici su sistemi ed applicazioni ad alto rischio
- **Analisi degli scenari:** identificazione superficie e tecniche di attacco



Transizione PQC - Dati rilevanti per il cryptography inventory

CREDEM

BANCA

Cryptography Data

- **Protocolli**
- **Cipher suite, algoritmi di crittografia e funzioni di hashing**
- **Mapping dei certificati**
- **Chiavi crittografiche**
- **Librerie e dipendenze**
- **Standard crittografici**



Application Data

- **Tecnologia di riferimento:** codice e tipo di data storage
- **Tipologia applicazioni:** Web, Mobile, LLM/GenAI, Cloud native, Client-Server, Mainframe
- **Tipo di deployment:** On prem, Cloud tenant, Mainframe, Code repository, Container image
- **Ciclo di vita**
- **Indice di rischio**



Threat modeling Data

- **Scopo della crittografia:** relazione con le tecniche di attacco
- **Superficie di attacco**
- **Classificazione e retention dei dati**



3

Hardening dei meccanismi di autenticazione

- Adozione hashing post-quantistico **SPHINCS+**
- Abilitazione nuovi meccanismi di autenticazione (es. estensione MFA con biometria, soluzioni passwordless)
- Utilizzo di funzioni di derivazione delle chiavi (KDF, Key Derivation Functions)

4

Sostituzione algoritmi vulnerabili

Integrazione ed utilizzo di soluzioni PQC per la progressiva sostituzione degli algoritmi vulnerabili con quelli approvati

- **ML-KEM** (Crystals–Kyber) basato su crittografia reticolare
- **ML-DSA** (Crystals–Dilithium) basato su crittografia reticolare
- Utilizzo di **SPHINCS+** per firma digitale
- Aumento dimensione chiavi per crittografia simmetrica (**AES**)

Requisiti specifici per architetture crypto-agili

CREDEM

BANCA

Discovery automatico

Monitoraggio continuo della crittografia
mediante strumenti specifici

Integrazione con Cryptography inventory

Astrazione crittografica

Disaccoppiamento tra business logic e librerie
crittografiche mediante meccanismi di
astrazione per favorire i processi di incident
response in caso di nuove minacce quantistiche
e per adottare algoritmi quantum-safe
preservando la continuità operativa senza
intervenire sul codice applicativo

Supporto ibrido e multi-algoritmico

Supporto coesistenza di algoritmi tradizionali e
algoritmi di crittografia quantum-safe

Automazione

Esecuzione automatica dei test crittografici
(crittoanalisi, performance e verifica delle
chiavi)