PQC Risk Assessment: Measuring Adoption

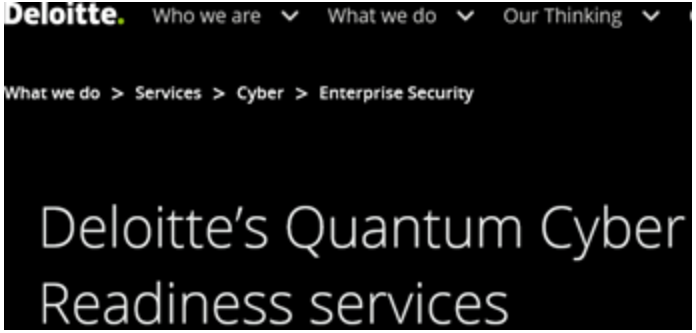
June 18, 2025

Anita Nikolich & Phuong Cao

ILLINOIS
NCSA | National Center for Supercomputing Applications

THALES
Building a future we can all trust

Are You Post-Quantum Ready?



Forbes

Inside The Coming Quantum Crisis: Why CEOs Must Prepare For Q-Day Now

THALES
Building a future we can all trust

Are You Post-Qu

Forbe

Inside The Coming Qu
Must Prepare For Q-D

Who we are | What we do | Our Thinking

Services > Cyber > Enterprise Security

bitte's Quantum Cyber
diness services

ISACA

5 / Volume 10 / How to Conduct a Quantum Risk Assessment Using IS

tum Risk Assessment
amework

Risk: Harvest Now, Decrypt Later (HNDL)

Stolen Data

Encrypted, sensitive data and password vaults decrypted when quantum computers break classical algorithms.

Data in Transit

Encrypted (https) traffic is recorded now and decrypted when quantum computers break classical algorithms.

PQC Migration Roadmap (2025 - 2035)

Cryptographic Asset Inventory & Data Inventory

Threat Modeling: attack surface, data types, dependency analysis

Incorporate Quantum into current Risk Assessments

Cost Analysis of PQC Migration

Prioritize by Risk

What is a Cryptographic Asset Inventory?

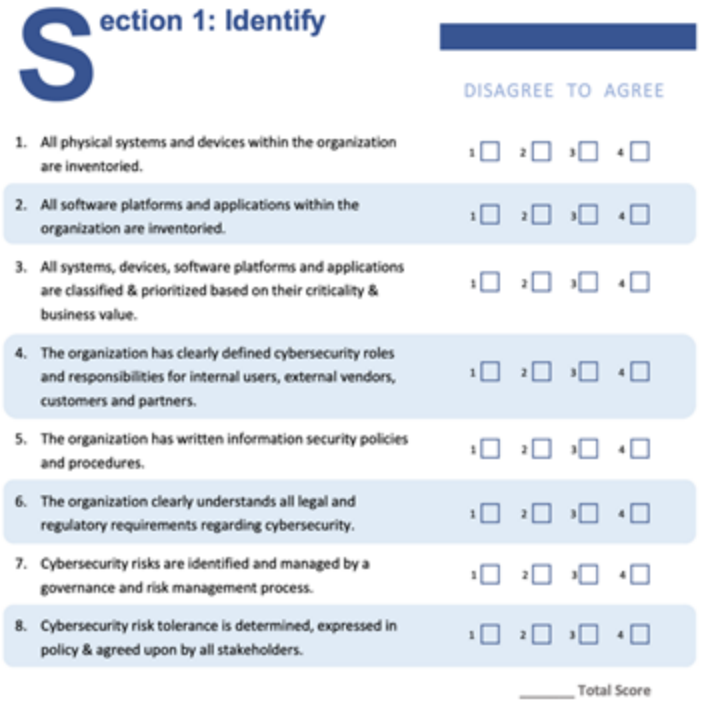
- Hardware (models, manufacturers) and protocols used
- Operating Systems, vendors, products, and versions
- Enterprise Applications (and crypto keys used)
- Data being encrypted by the organization
- List of 3rd party vendors (do they manage all keys? some keys?)

Why Should You Care?

Many insurance companies are beginning to include PQC readiness questions in risk questionnaires.

Underwriters are developing new risk models for PQC attacks.

Most recommend doing internal audits ASAP.



Section 1: Identify

DISAGREE TO AGREE

1. All physical systems and devices within the organization are inventoried. 1 2 3 4
2. All software platforms and applications within the organization are inventoried. 1 2 3 4
3. All systems, devices, software platforms and applications are classified & prioritized based on their criticality & business value. 1 2 3 4
4. The organization has clearly defined cybersecurity roles and responsibilities for internal users, external vendors, customers and partners. 1 2 3 4
5. The organization has written information security policies and procedures. 1 2 3 4
6. The organization clearly understands all legal and regulatory requirements regarding cybersecurity. 1 2 3 4
7. Cybersecurity risks are identified and managed by a governance and risk management process. 1 2 3 4
8. Cybersecurity risk tolerance is determined, expressed in policy & agreed upon by all stakeholders. 1 2 3 4

_____ Total Score

PQSee:

A Free Software Tool for PQC Network Protocol Assessments

Classical Algorithms: Example Uses

RSA:

Digital Certificates (many banks still use RSA certs)

SSH & TLS to authenticate servers & clients

Elliptic Curve Cryptography (ECC)/ECDSA

Bitcoin key generation & transactions

AES-256:

AWS

Windows OS

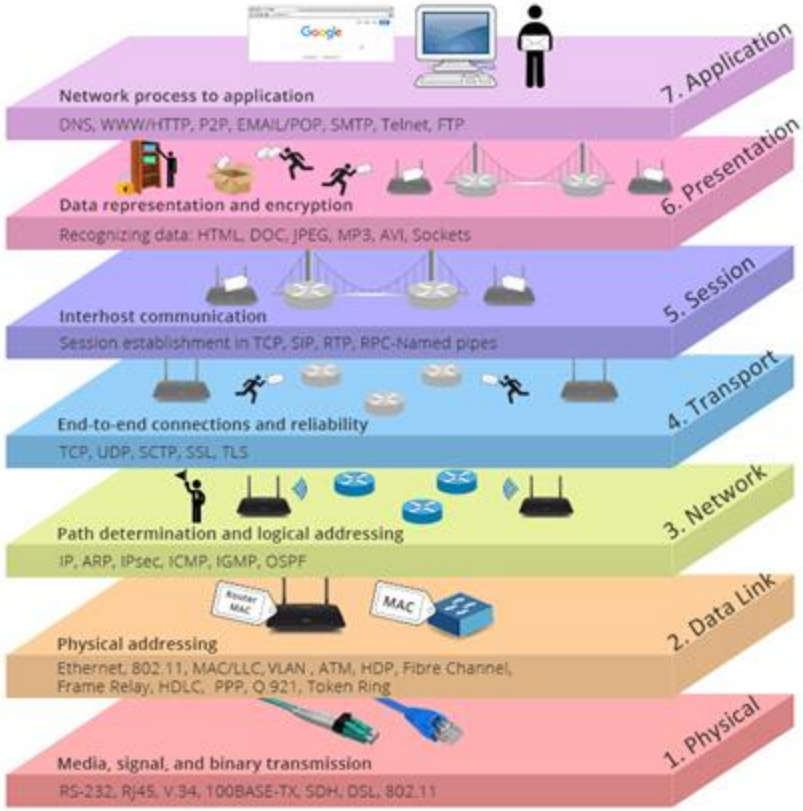
Hash Functions - **SHA-2 or 3**:

IOT devices

What does PQSee Help Inventory?

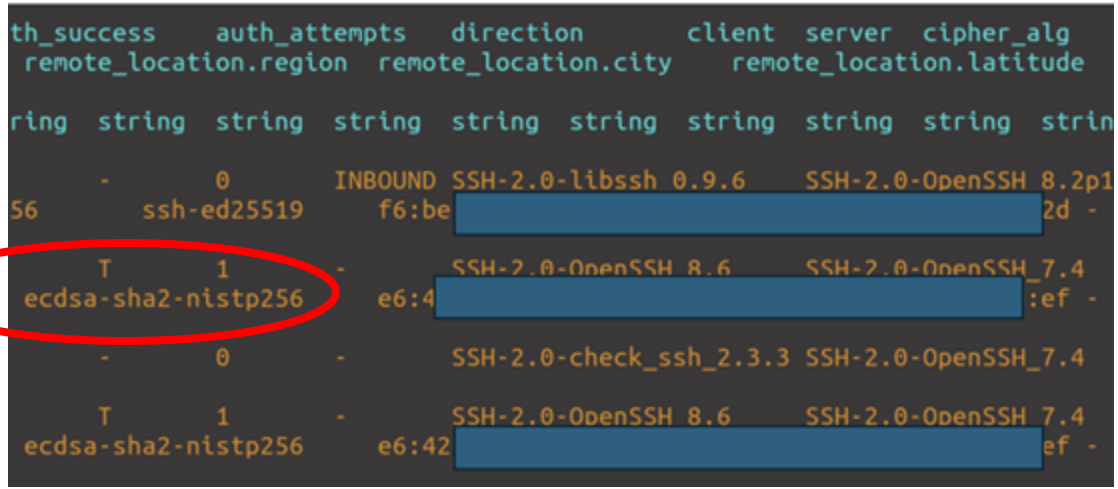
- Layer 7: Application layer
  - Remote Desktop Protocol (RDP)
  - Domain Name System (DNS)
  - Secure Shell (SSH)

- Layer 4: Transport layer
  - Transport Layer Security (TLS)

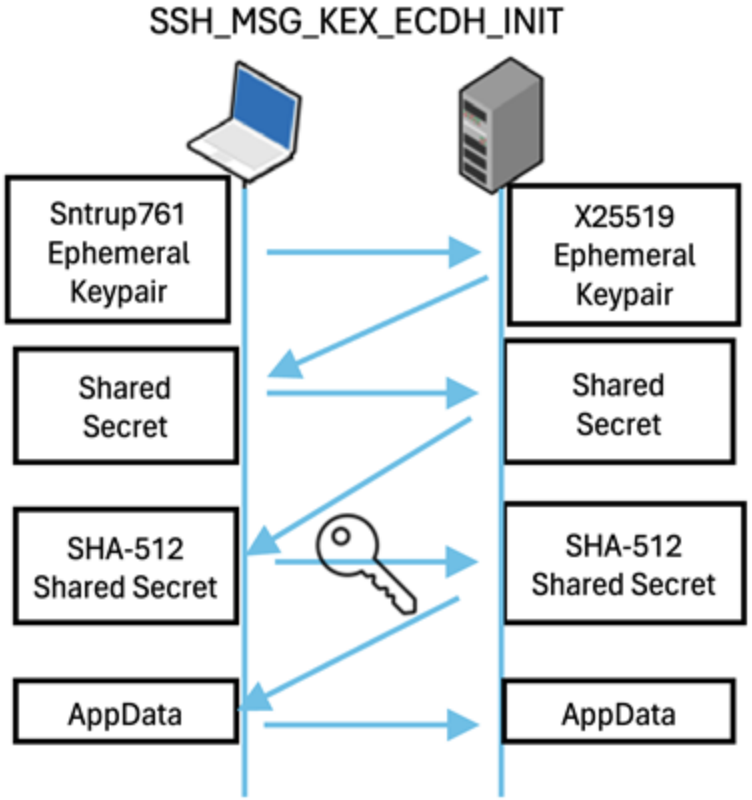


How Does PQSee Work?

- Takes your Intrusion Detection (Zeek) or network data
- Identifies cryptographic handshake for SSH, TLS and more
- Handshake data indicates whether it's PQC compliant



Current PQC implementation in SSH



PQC Adoption among Vendors

2024
RISC-V with PQC support proposed in NASA's future missions

Apr 2025
OpenSSL 3.5 PQC support

May 2025
Windows 11 PQC support

May 2025
AWS supports PQC in SFTP file transfers

Current and Future Work

Data Curation

Security Data Lake @ NCSA

Anonymized PQSee data and/or results from partners

Security Monitoring

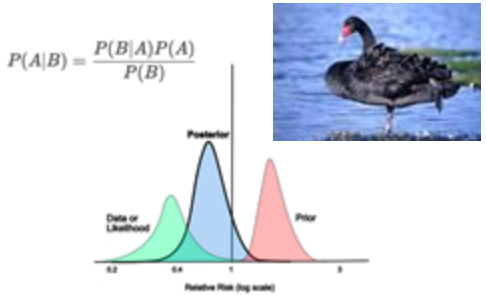
zeek

In-house Zeek experts and clusters

Work with Zeek community

- Zeek plugin for PQC statistics
- PQC-aware Zeek parser
- Develop customized sensors for new attacks

Risk Assessment



Estimating the posterior probability

- Catastrophic, blackswan, wide-spread disruption events.
- Impact assessments

=> Assisting UIUC CISO with PQC risk assessment

How We Can Help

- Follow up technical call for those who want help setting up PQSee or want to know technical details
- Upload your sanitized packet captures - we can help analyze them: put them on your own storage or our secure storage
- Ask us how to help your risk assessment process!

- Join our mailing list: pqsee@lists.illinois.edu
- Get PQSee at: https://github.com/pmcao/pqsee

Phuong Cao
pcao3@illinois.edu
https://github.com/pmcao/pqsee

Anita Nikolich
anitan@illinois.edu
www.neuralnetworks.com

ILLINOIS
NCSA | National Center for
Supercomputing Applications