Plan, Do, Check, Act
For Identity Protection on a Global Scale

https://quant-x-sec.com | xb@quant-x-sec.com
Image Source: Midjourney

QUANT-X SECURITY & CODING

mastering digital complexity

Who We are

IT EXPERTS / CONSULTING

- Information Security
- Project Management
- Software Engineering
- IT Operations

RESEARCH & DEVELOPMENT

- Software Engineering
- Security Analyses & Proofs

Image Source: Midjourney

xb@quant-x-sec.com

Quantum Technology Related Activities

"Preserve confidentiality, integrity and availability of data in the future"

- Quantum and Post-Quantum Security Integration
- Quantum and Post-Quantum Security Migration
- Project Management for Infrastructure Changes
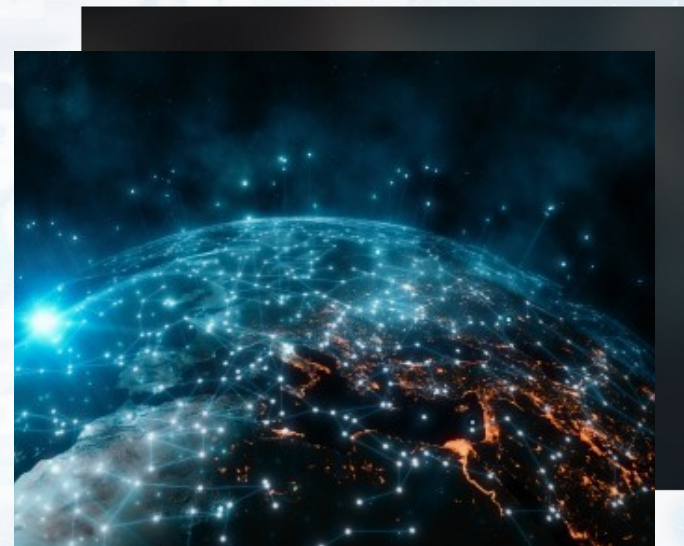- Quantum Security Proofs and Validation

Image Source: iStock

xb@quant-x-sec.com

3

Today's Focus: Quantum and Post-Quantum Integration

QUANTUM SECURE DIGITAL IDENTITIES

https://quant-id.de/

QUANT-X SECURITY & CODING   Fraunhofer IPMS   MTG   UR Universität Regensburg

QUANT-ID *"QRNG Entropy and Post-Quantum Security for globally used IAM Protocols"*

FACTS

- Usage of cloud infrastructures → web protocols for Identity Access Management (IAM)

- Most cyber attacks are based on some identity misusage (PAs and NPAs)

- Infrastructure providers implement Information Security Management Systems to maintain digital security (ISMS)

- IAM protocol designers and analysts continuously assess protocol design and implementations to maintain security

Image Source: iStock

xb@quant-x-sec.com

5

Plan, Do, Check, Act

INFRASTRUCTURE PROVIDERS REGULATED ORGANISATIONS

Governance, Operations, Auditing

- Account Management (PAs and NPAs)
- Authentication and Authorization
- Secure Configuration
- Connectivity
- Patch Management
- Malware Resilience
- Lifecycle Management
- Cryptography
- Vulnerability Scans
- Penetration Tests
- Red and Blue Teaming
- Security Event Monitoring
- Threat Intelligence
- Change Management
- DDoS and APT Resilience
- 3rd Party Security
- …

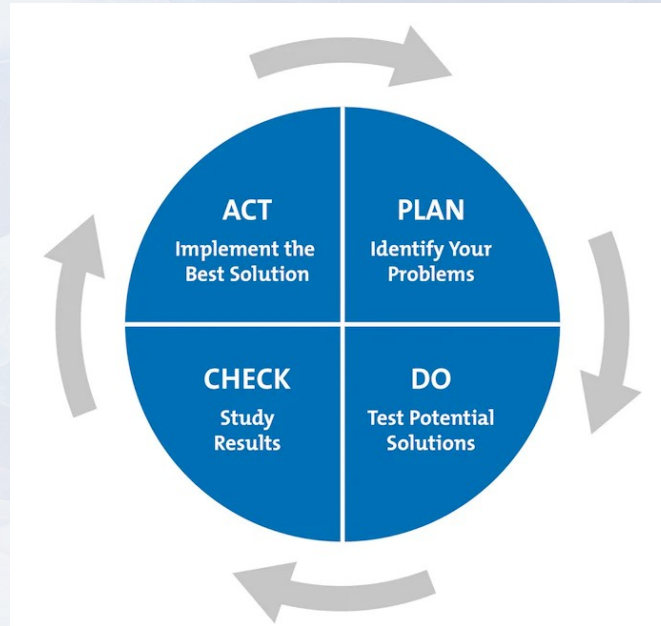*image source: https://www.mindtools.com/*

IAM PROTOCOL DESIGNERS AND ANALYSTS

E. g. OAuth History

- OAuth Core 1.0 release: 4 Dec 2007
- OAuth 1.0 RFC 5849: April 2010
- OAuth 2.0 RFC 6749: Oct 2012

Global OAuth security experts continuously engage in

- Research
- Working groups for new protocols in the protocol family (incl. OpenID Connect)
- RFC updates and design
- Threat modeling
- Formal analyses
- Implementation checks
- Vulnerability assessments

10/08/23

xb@quant-x-sec.com

6

Yearly Workshops

xb@quant-x-sec.com

Yearly OAuth Security Workshops

PRESENTATIONS

Why the trust model of OIDC is broken

Full disclosure: behind the scenes of SD-JWT (selective disclosure - JSON Web Token)

Defending Against Cross-Device Consent Phishing Attacks

Formal Analysis of FAPI 2.0 and the OAuth Device Authorization Grant

Beyond Scopes: RAR in the Real World

How to build interoperable decentralized identity systems with OpenID for Verifiable Credentials

OAuth 2.1

High-security & interoperable OAuth 2: What's the latest?

A Key Is Not Enough: OpenID Connect Federation 1.0

Formal Verification of the Cedar Policy Language

Programming Engineers: How Standards Shape the Way We Work

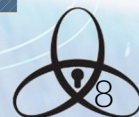Identity Theft using In-Browser Communications in Dual-Window Single Sign-On

OAuth 2.0 Redirect URI Validation Falls Short, Literally

What should a secure standards framework for Machine Identities look like?

…

Looking forward to international Quantum security workshops on established and new Quantum security standards!

xb@quant-x-sec.com

8

Quantum and Post-Quantum Security

OAuth / OpenID Connect

Thank you!
Questions?
https://quant-x-sec.com | xb@quant-x-sec.com

10/08/23

xb@quant-x-sec.com

QUANT-X SECURITY & CODING

mastering digital complexity