Identity Access Security with Quantum Entropy

How we enable the integration of quantum technologies in classical infrastructures

image source: midjourney

xb@quant-x-sec.com

03/19/24

Who We are

Founded in 2019 | Located at Hanover, Germany | 8 employees: Men and Women of Letters

IT EXPERTS / CONSULTING

- Information Security
- Project Management
- Software Engineering
- IT Operations (Linux & Full Stack Web)

RESEARCH & DEVELOPMENT

- Software Engineering
- Security Analyses & Proofs

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
- Quantum Security Proofs and Validation
- Quantum Algorithm Feasibility Studies

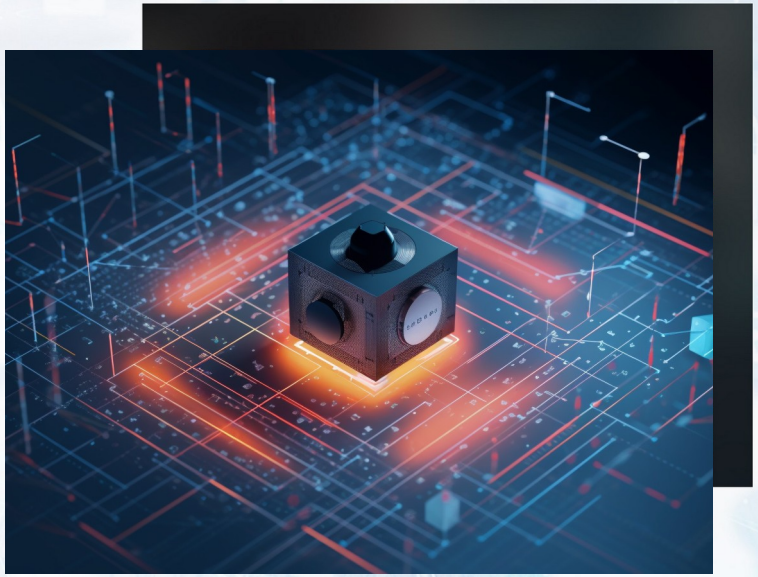


image source: midjourney

xb@quant-x-sec.com

R&D - Quantum and Post-Quantum Integration

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

Dieses Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KISQ108K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei Quant-ID.

Fraunhofer IPMS · MTG · Universität Regensburg

image source: iStock

Why Identity Access Management (IAM)?

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

FACTS

- Usage of cloud and IOT → web protocols for Identity Access Management (IAM)
- Most cyber attacks are based on some identity misusage (person, device or application account)
- IAM protocol designers and analysts continuously assess designs and implementations to maintain security
- High Entropy is essential for access security!

Image Source: iStock

xb@quant-x-sec.com

Attacks on SSH Port of a New Born VM in the Internet

2) Check Hacking Attempts

You will see all hacking attempts on the VM. Therefore we need to configure the VM such that these attempts will be reduced and cannot be successful. Note the frequency of these attempts!!!

```
 sudo nano /var/log/auth.log

Example output:
Sep 10 02:05:00 h3004228 sshd[418705]: Failed password for invalid user contador from 49.113.85.117 port 58987 ssh2
Sep 10 02:05:02 h3004228 sshd[418705]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:04 h3004228 sshd[418705]: Failed password for invalid user contador from 49.113.85.117 port 58987 ssh2
Sep 10 02:05:07 h3004228 sshd[418705]: Received disconnect from 49.113.85.117 port 58987:11: disconnected by user [preauth]
Sep 10 02:05:07 h3004228 sshd[418705]: Disconnected from invalid user contador 49.113.85.117 port 58987 [preauth]
Sep 10 02:05:07 h3004228 sshd[418705]: PAM 2 more authentication failures; logname= uid=0 euid=0 tty=ssh ruser= rhost=49.113.85.117
Sep 10 02:05:11 h3004228 sshd[418715]: Invalid user ubuntu from 49.113.85.117 port 10311
Sep 10 02:05:11 h3004228 sshd[418715]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:11 h3004228 sshd[418715]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=49.113.85.117
Sep 10 02:05:13 h3004228 sshd[418715]: Failed password for invalid user ubuntu from 49.113.85.117 port 10311 ssh2
Sep 10 02:05:13 h3004228 sshd[418715]: pam_unix(sshd:auth): check pass; user unknown
Sep 10 02:05:16 h3004228 sshd[418715]: Failed password for invalid user ubuntu from 49.113.85.117 port 10311 ssh2
Sep 10 02:05:17 h3004228 sshd[418719]: Invalid user admin from 141.98.11.11 port 22378
Sep 10 02:05:17 h3004228 sshd[418719]: pam_unix(sshd:auth): check pass; user unknown
...

More ways to check:
grep "Failed password for root" /var/log/auth.log

```

China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
China (CN)
Lithuania (LT)

Top Banned IP Addresses on a Day in February

# Bans	IP Address	Country	City	ISP
56	185.161.248.184	Russia	Moskau	Kisara LLC
33	91.238.181.247	France	Paris	Layer7 Networks GmbH
29	185.161.248.183	Russia	Moskau	Kisara LLC
18	45.175.100.75	Argentina	San Juan	Rodriguez Martinez Jose Nicolas
14	89.208.106.218	Netherlands	Amsterdam	Aeza International LTD
12	81.17.21.234	Switzerland	Zürich	Private Layer Inc
11	185.217.1.246	Sweden	Stockholm	W1N Ltd
9	43.156.34.165	Singapore	Singapore	Aceville Pte.Ltd.
8	129.226.215.152	Singapore	Singapore	Tencent Cloud Computing (Beijing) Co. Ltd.
8	13.74.46.65	Ireland	Dublin	Microsoft Corporation
8	165.22.69.77	Germany	Frankfurt Main	DigitalOcean LLC
8	165.227.166.247	Germany	Frankfurt Main	DigitalOcean LLC
8	92.119.231.76	Ukraine	Kherson	IPX – FZCO, AS58066 Gutkin Vladyslav

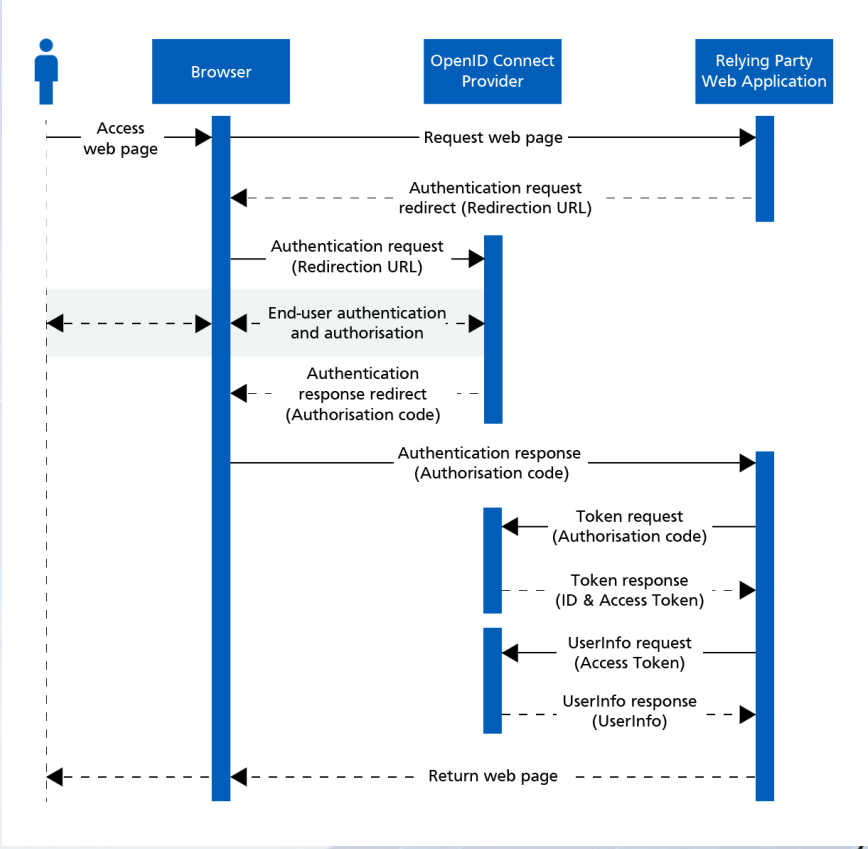
OAuth and OpenID Connect

RFC history

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

Founded in 2007, the OpenID Foundation (OIDF) is a non-profit open standards body developing identity and security specifications that serve billions of consumers across millions of applications.

8 x entropy in a simple authorization code flow access!



Source: UK National Health Service

OAuth 2.0 and OpenID Connect

OAuth experts continuously engage in

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

Cryptography and entropy are context topics!

QUANT-ID

Dieses Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 16KISQ108K gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt bei Quant-ID.

Associated
- ROLAND HEDBERG
- GUISEPPE DE MARCO
- DB

Fraunhofer IPMS:
QRNG development

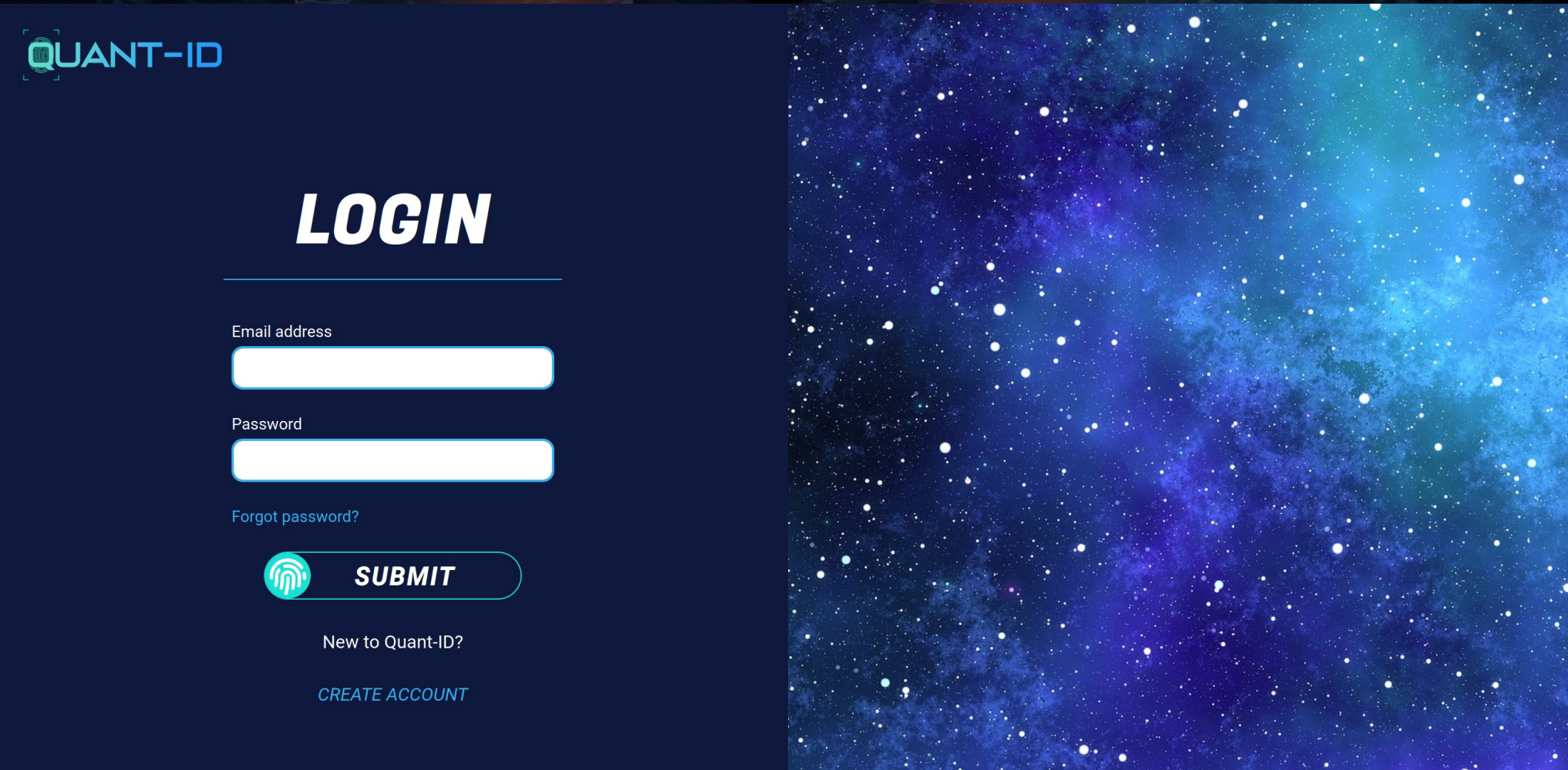
Quant-X:
Project coordination
IAM protocol adjustments
Quant-ID provider and clients
QRNG entropy validation
Statistics

MTG AG:
PQC-PKI
HW-SW APIs

University of Regensburg:
PQC-Analyses
QRNG entropy proof and validation lead

xb@quant-x-sec.com

Quant-ID Provider



Contact us if you are interested in a cooperation.

Thank you! Questions?

https://quant-x-sec.com

03/19/24

xb@quant-x-sec.com