XIPHERA

CRYPTOGRAPHY UNDER THE HOOD WEBINAR SERIES

Fortifying Digital Resilience

Security Foundations for IoT, AI, and Cloud Systems

Petri Jehkonen

Director of
Strategic Programs

Xiphera

Agenda

I. Industrial landscape

II. Security elements for digital resilience

III. Resilience with system of systems

IV. Example solutions for digital resilience in IoT, AI, and Cloud

Industrial Landscape

Digitalisation continues

Connectivity increases

System complexity expands

Platforms & data domains diffuse

Value of AI models and data grows

Advanced data breaches and attacks multiply

The growth of IoT, cloud, and AI solutions is exponential.

→ Business demands significant scalability

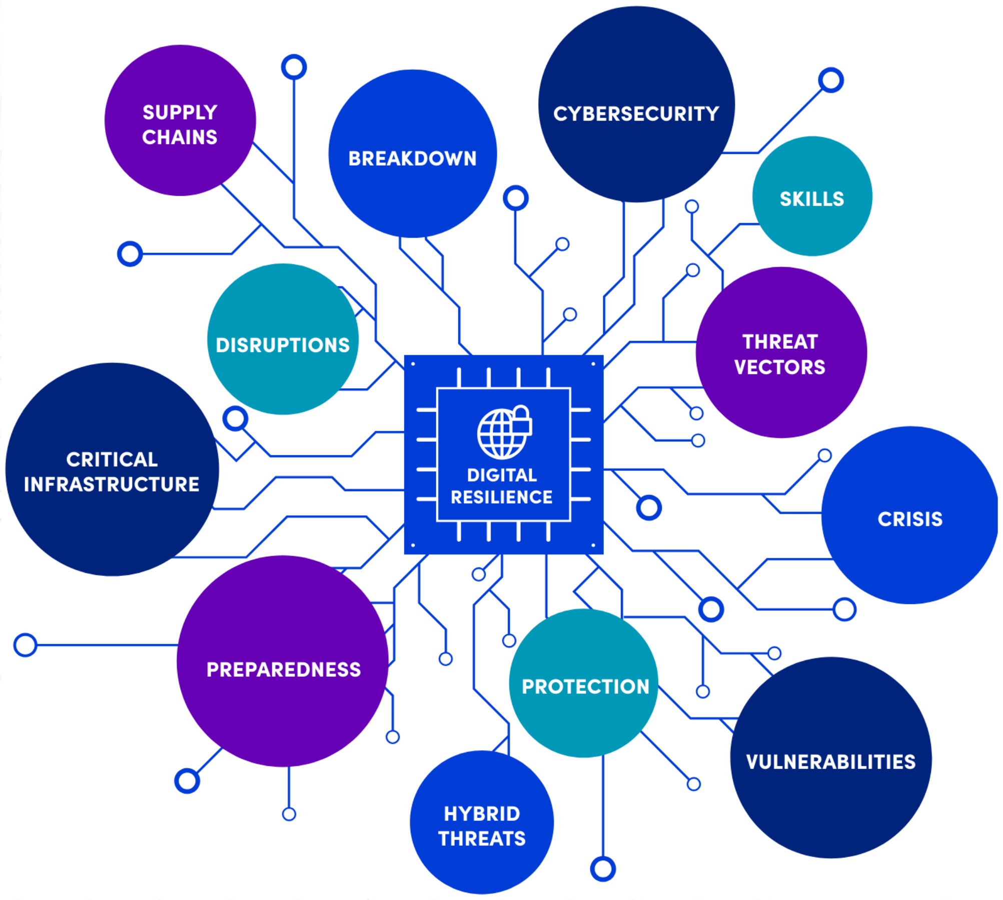
→ Security of **system of systems** is harder to guarantee

→ Security still seems to be a secondary priority in system design

The demand to match market needs leads to extremely high pressure for fast service development cycles.

→ Insufficient security of the underlying infrastructures increases the risks for digital resilience

Security Elements for Digital Resilience



Digitaleurope.org: The Digital Front Line – 15 actions to boost Europe's Digital Resilience

- Building the **digital trust** on system of systems needs to be built on several levels
- Requirement to have defence in depth in systems leads to requirement to have **digital resilience**
- Digital resilience **requires** digital trust
- Customisation and selecting **right** security elements and parameters for a solution
- Agility to respond to changing security requirements is mandatory

Resilience within System of Systems

- IoT, IIoT, cloud and AI services are modern examples of solutions operating on system of systems
- Supply chain is the basis of trust

Foundations of digital resilience is built on validated system components

- Secure elements need to be used securely
- Example solutions:
  1. *Secured boot*
  2. *Hardware Root-of-Trust*
  3. *Confidential Computing*
  4. *Secured AI*

Example Solutions for Digital Resilience in IoT, AI, and Cloud

Secured Boot

- Protecting system power-up sequence
- Verify the authenticity and integrity of system boot-image
- Increasing digital resilience for system power-up:
  - Cryptographically secured boot-image
  - Trusted tool to create signature for boot-image
  - CPU/Semiconductor device able to perform verification of boot-image during power-up

Hardware Root-of-Trust

- Vulnerabilities may originate from design, operating system, CPU, support libraries…
- The hardware platform needs solid Root-of-Trust (RoT) for computing system
- Hardware RoT offers
  - Service to authenticate, encrypt and decrypt software
  - Ability to manage digital identities
  - Cryptographic key generation and management, including ephemeral keys
  - Secured boot is inherently required
- Ease of validation and certification is important!

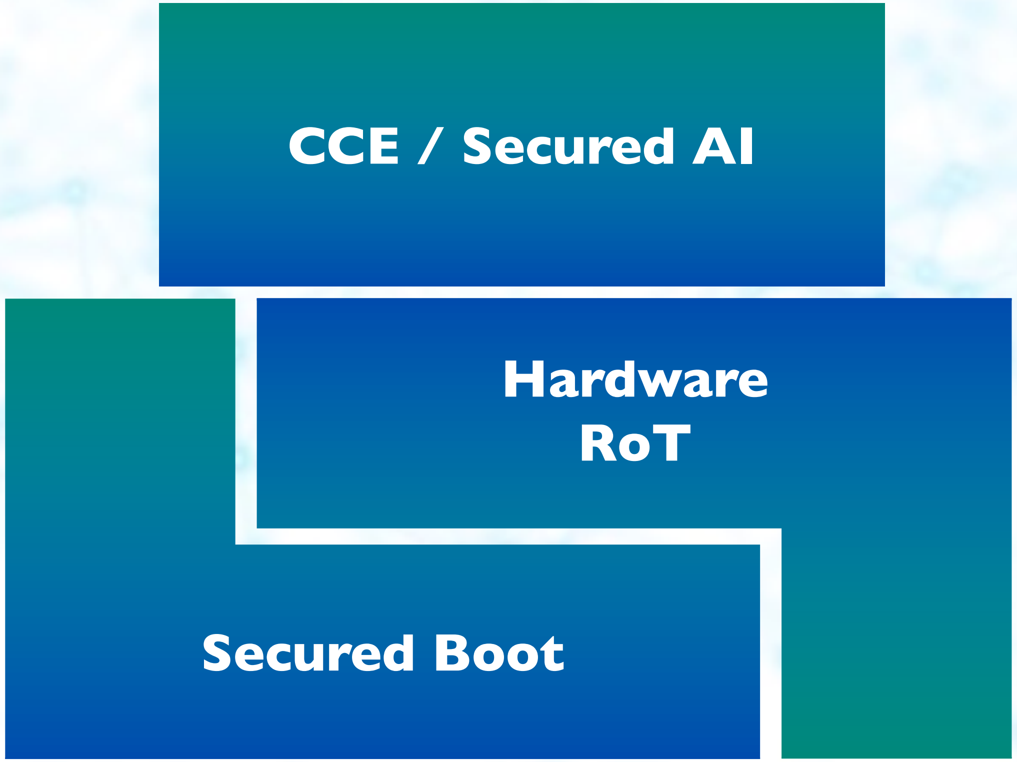
Confidential Computing Engine

- Secured boot and Hardware RoT are used for securely deploy application to the confidential computing enclave
- Confidential computing environment should offer absolute isolation of code and data between applications
- Existing trusted execution environments (TEE) have notable vulnerabilities both on hardware and software
- Xiphera’s nQrux™ Confidential Computing Engine (CCE) is a customisable solution offering isolation and protection for both code and data from the rest of the system

Secured AI inside CCE

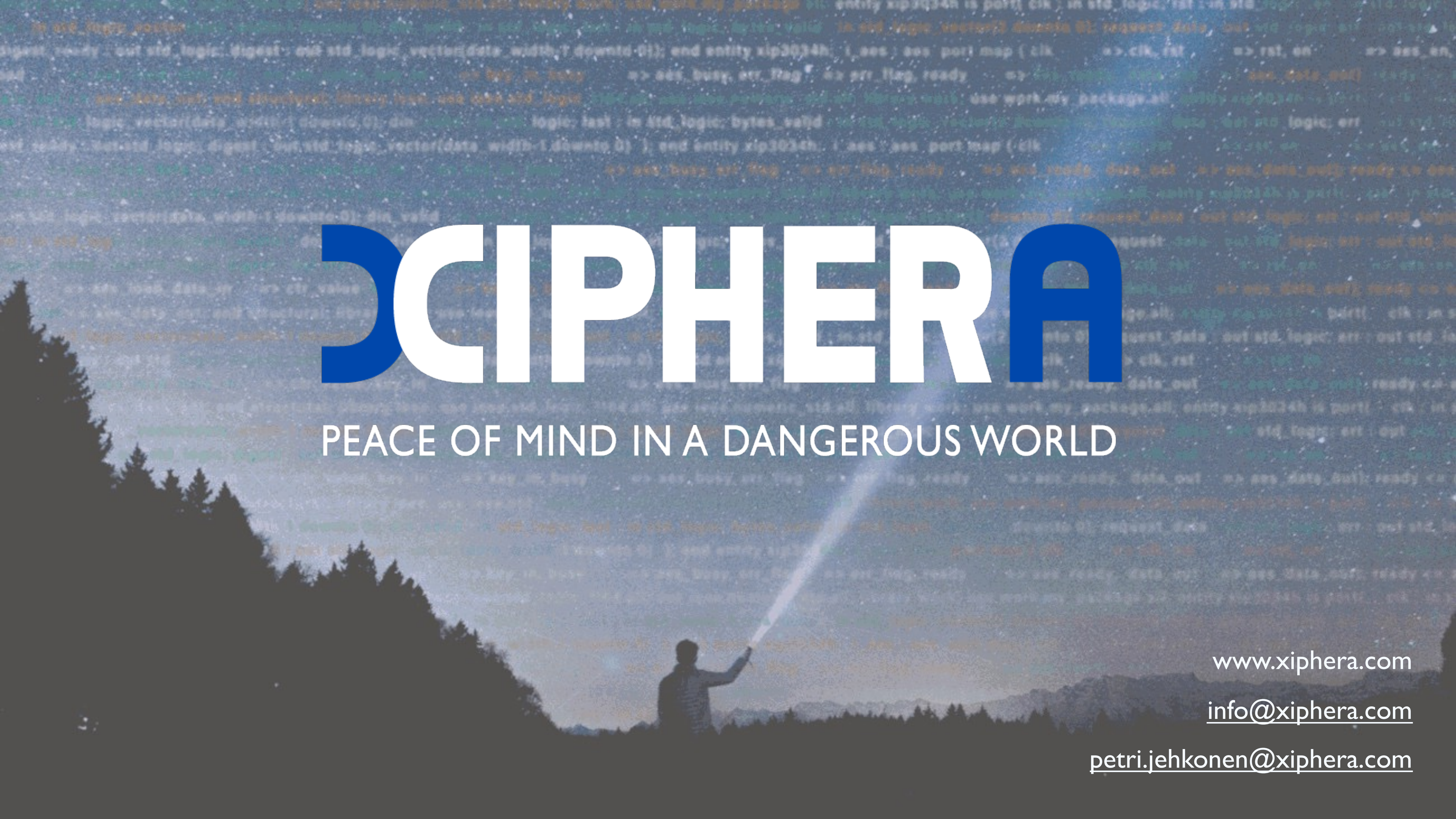
- How to secure AI and ML models and data?
- Development of system elements is to be trusted
- The system elements are to be trusted
    - The computing platform is secured
    - The AI model deployment is secured
    - The computing environment is isolated from the rest of the system
- Electro-physical isolation of AI model and data!

Foundations for Digital Resilience



- Modern IoT, Cloud and AI can be protected
- Digital resilience requires digital trust
- Creating resilience starts with validated trusted **hardware** elements, which need to be used secure
- Services and solutions are typically **customised** based on purposes and requirements

Xiphera's nQrux™ Hardware Trust Engines offer a toolkit of customisable security solutions for IoT, AI, and cloud environments.



XIPHERA

PEACE OF MIND IN A DANGEROUS WORLD

www.xiphera.com

info@xiphera.com

petri.jehkonen@xiphera.com