Security Research and Practices on Zero Trust for Software Supply Chain in Computing Force Network

Chen ZHANG, China Mobile
Associate Rapporteur of Q15/17

28 August 2023

01

Software Supply Chain Security Challenges in Computing Force Network

02

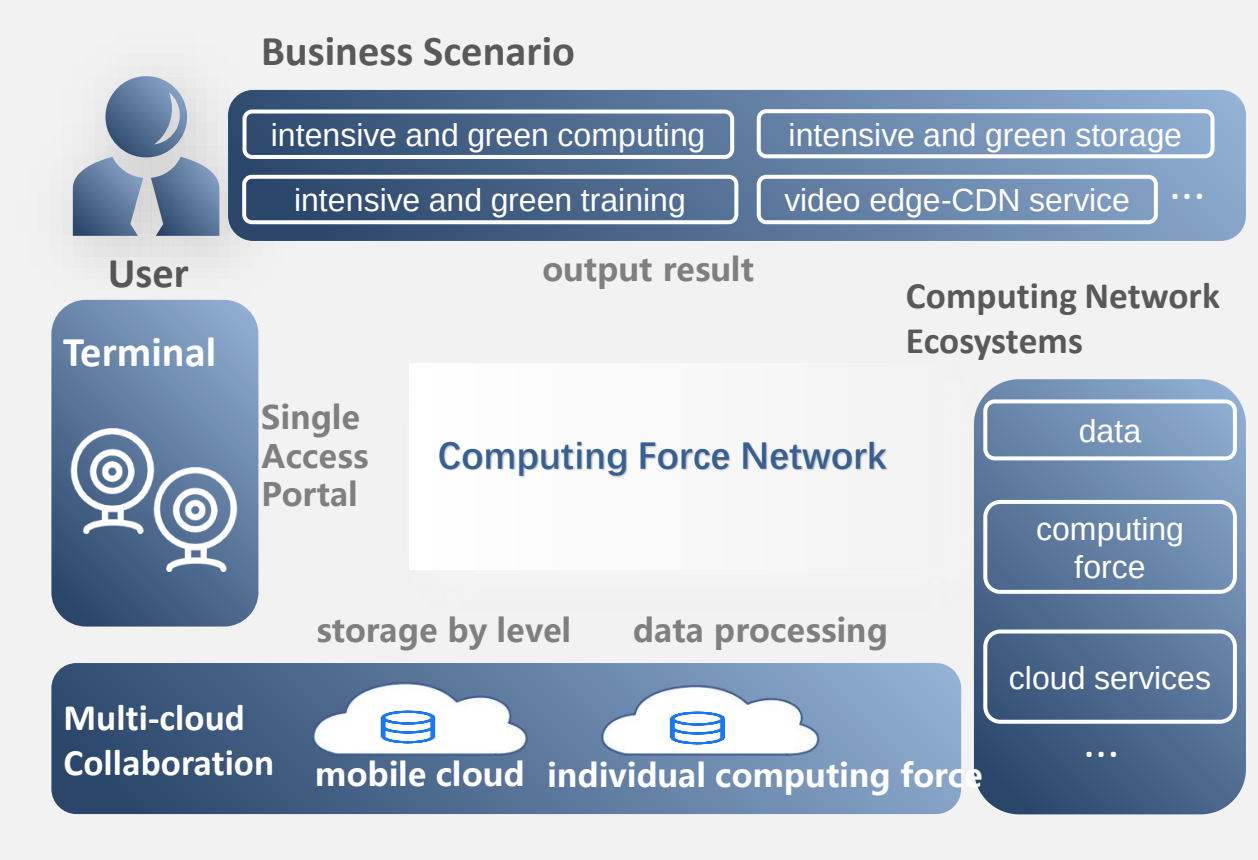
Security Research and Practices of Software Supply Chain Based on Zero Trust

01

Software Supply Chain Security Challenges in Computing Force Network

FIRST PART

Computing Force Network



Computing force network (CFN) is proposed by China Mobile, the basic principles of which are in line with CNC.

Computing force network is a kind of next generation of telecommunication-level information infrastructure that flexibly schedules and merges computing resources, storage resources, and network resources among cloud, edge, and terminal based on business requirements & models.

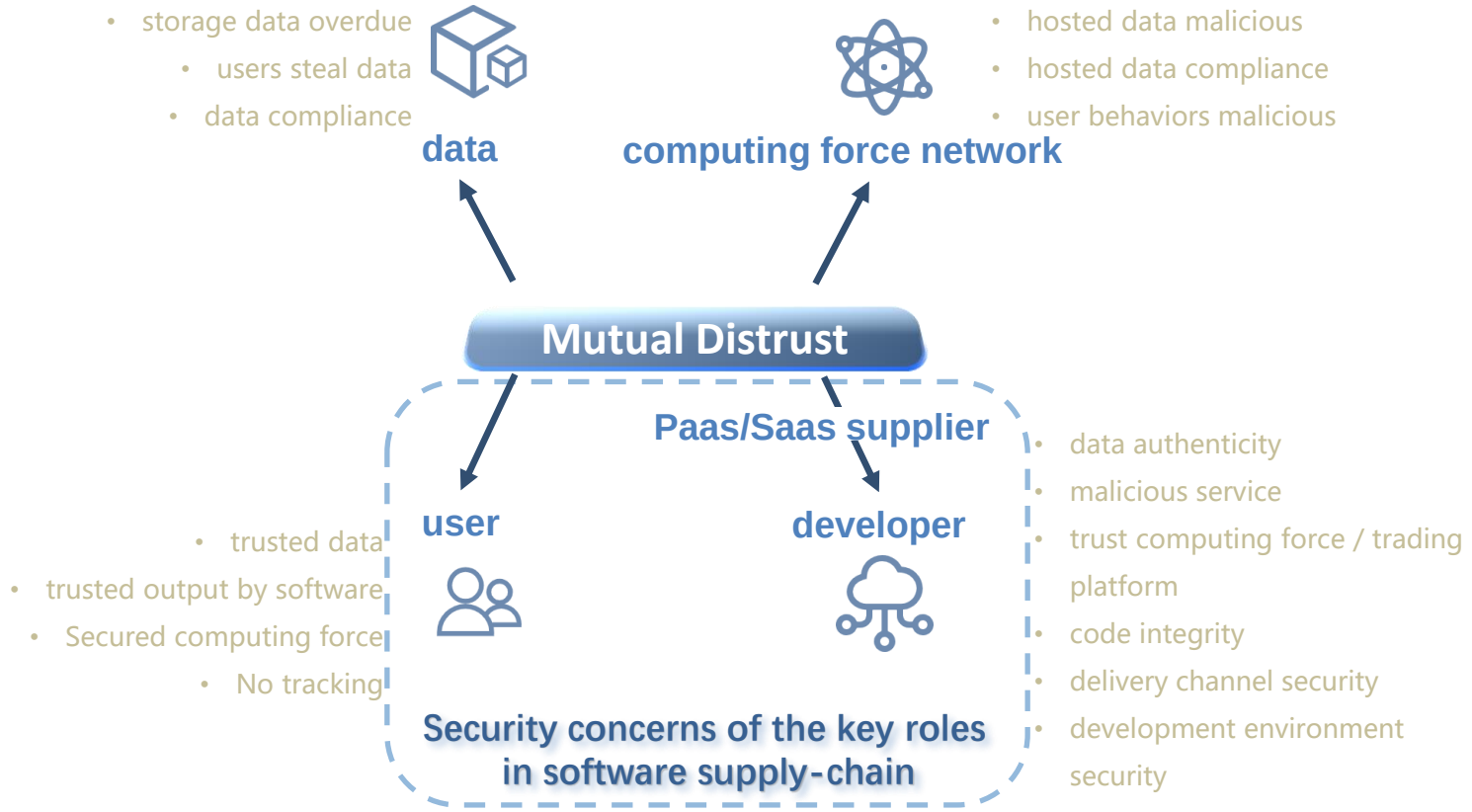
Software Supply Chain and Common Risks

Loose Definition

Software supply chain means software that an enterprise relies on, including software that is used for various activities such as research and development, operation, sales, and any activities related to software evaluation, production, and distribution.

Strict Definition

Software supply chain focuses on lifecycle of software from creation to delivery, revolves around related entities and business links.



New Challenges against Software Supply Chain in Computing Force Network

Sparsely Distributed CFN resources & components

Computing force network uses decentralized technologies, managing multi-party's idle computing resources, which will expand the territory of software in the lifecycle and so do the territory of the security controls.

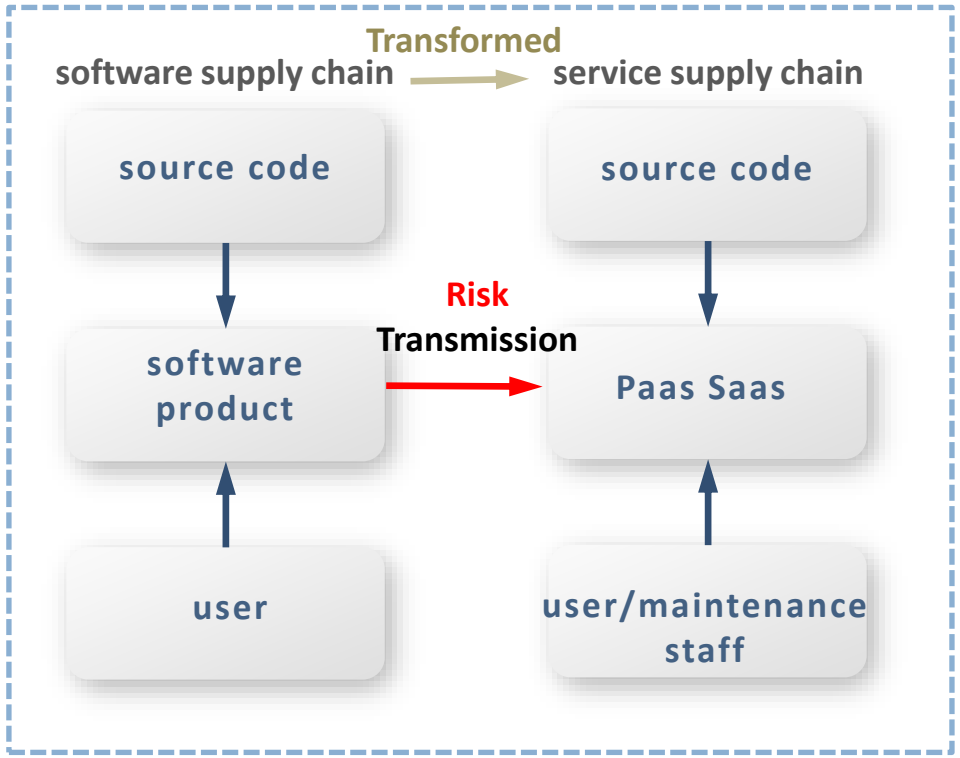
Heterogeneous platforms & Diverse hardware devices

Heterogeneous platforms and diversified hardware devices existing in cloud computing, edge computing, and terminal-side in CFN, drive the security management to trace the software supply-chain risks with the consideration of compatibility and differentiation carefully and widely.

Additional risks from service supply chain

Service is provided in the form of SaaS/Paas, and malicious user/maintenance personnel behavior can pose a security threat to the service, further affecting the software supply chain.

Distrust chain of Software Supply Chain in Computing Force Network



developer

- Third party component untrusted
- Developer untrusted

supplier

- Software untrusted
- Under Saas/Paas mode,user behavior untrusted
  - Under Saas/Paas mode, service supply chain risks that users generate could be transmitted to software supply chain when user accesses service.

user

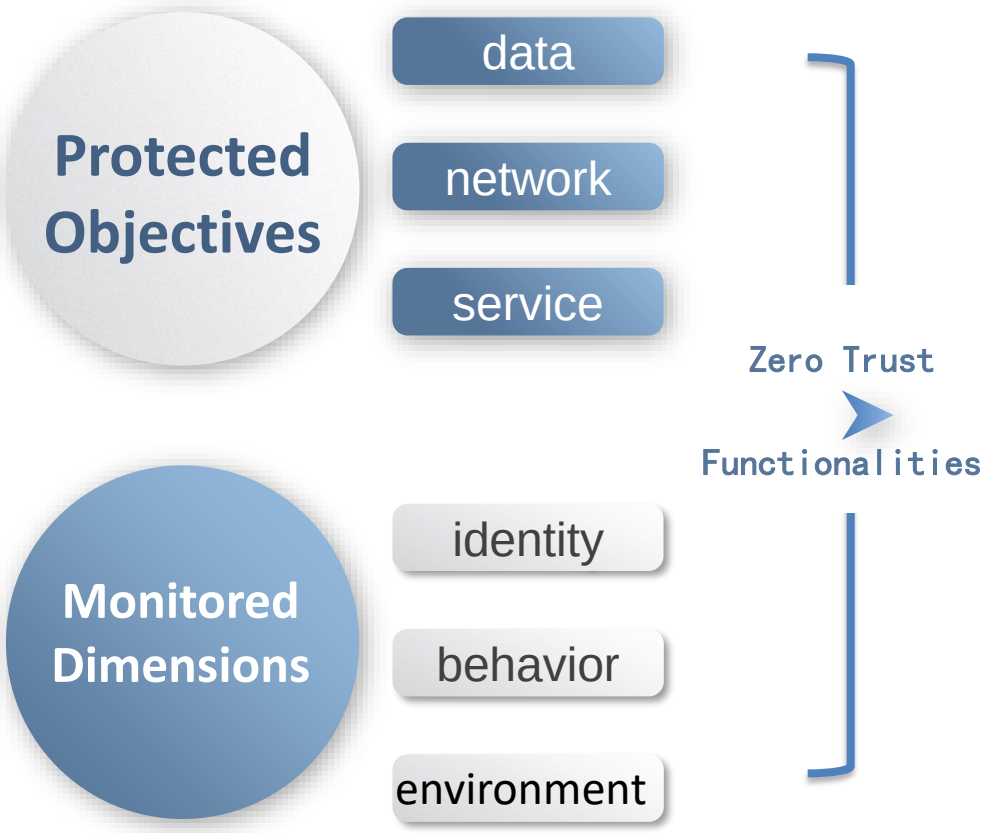
- Software untrusted
- Maintenance staff untrusted

Security Research and Practices of Software Supply Chain Based on Zero Trust

SECOND PART

02

Zero Trust Capability Framework



✓ Zero Trust ensures end-to-end security through continuous comprehensive risk control

✓ Zero Trust ensures the integrity of developer and user identities and behaviors

✓ Zero Trust ensures the security of the deployment and serving environments

✓ Zero Trust ensures the security of code/data/products hosting service.

✓ Zero Trust dynamically controls horizontal/vertical traffic and manages third-party components with fine-grained granularity

✓ Zero Trust validates the reliability of software delivery channels

Related Practices of Software Supply Chain Security in Industries

Trusted R&D Operations Security Capability Maturity Model

- Inheriting the core principles of SDL and DevSecOps
- Utilizing the advantages of SDL and DevSecOps frameworks
- Optimizing specific security practice elements

Cloud Security Shared Responsibility Model

- The security responsibilities shared by cloud service providers and customers are different
- CSPs need to take responsibility for ensuring physical security when customers use cloud services
- Customers need to take responsibility for ensuring that their solutions and data are securely identified, labeled, and correctly classified

Software Supply Chain Security Architecture based on Zero Trust

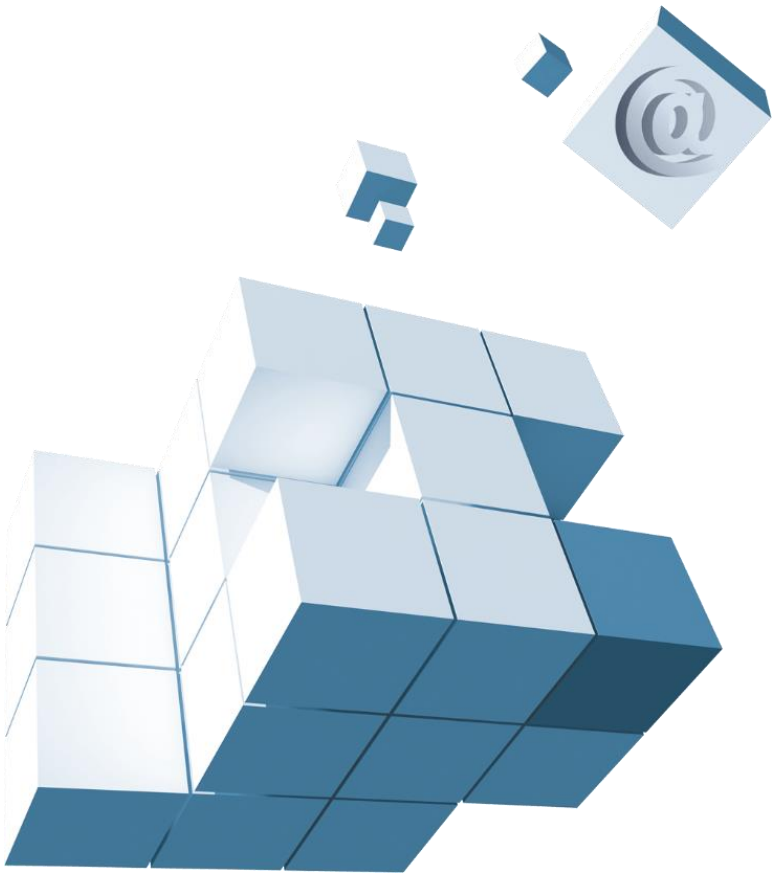
Zero Trust Security Architecture for Software Supply Chain

exposed surface concealment	continuous auditing	micro isolation	**trust endorsement**
reputation management	**trust challenge**	**supervision hosting**	**privacy computing**
remote trusted proof	principle of least privilege	equipment control	dynamic access control

risk detection of software code	risk detection of dependency on third-party component	software deliverables risk detection	risk detection of dependency on third-party services	Inspection of API of third-party services
• web vulnerability • logical vulnerability • data security	• component asset scan • component vulnerability detection • component license risk identification	• binary scan • mirror scan • library scan	• host asset scan • asset fingerprint scan • basic service vulnerability detection	API inspection of : • Payment • Unified Authentication • live streaming services • Data transportation • etc Supported by third parties

Secure data storage center

Key Capability of Zero Trust



Trust Challenge

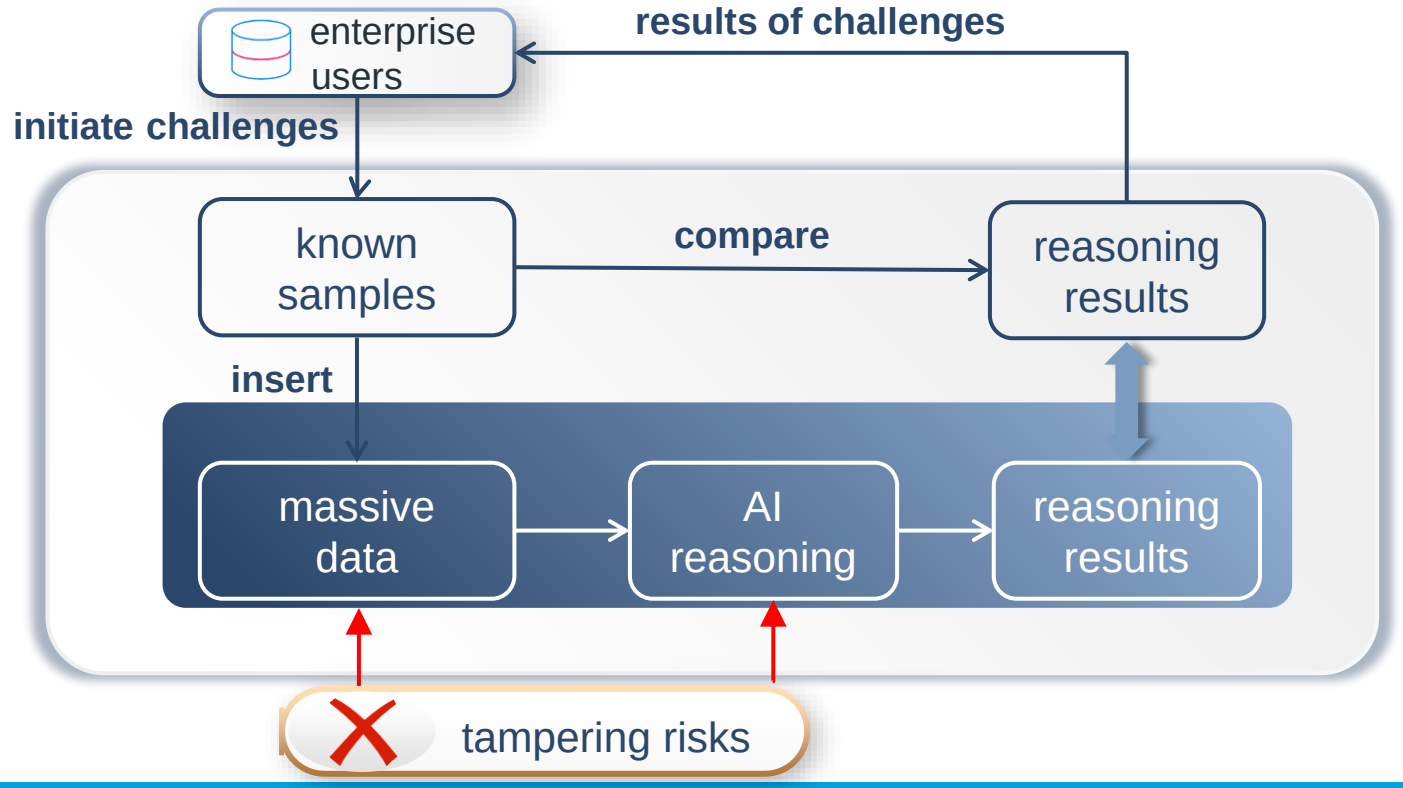
Randomly inserts verification tasks or data into a large number of computing tasks, or raises special computing problems, and judges whether the service results are credible based on the feedback from the service provider.

- **Redundancy of computational dimension**
- **Redundancy/duplication of computational task**
- **Redundancy/duplication of input data**
- **Challenge of typical problem**
- **Real person verification**

Reference Scenario for Trust Challenge

Data reasoning task: ensuring the consistency of input data and AI reasoning model is trustworthy.

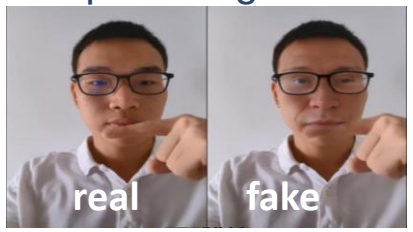
Trust challenge: ensuring the reasoning results of small, uniformly distributed samples align with previous anticipations.



Practice of Trust Challenge - Real Person Authentication

Designing video-based interactive challenges to target the vulnerabilities of deepfake algorithms

- Using different gestures to cover the face, aiming to expose more facial synthesis flaws.



Deepfake detection algorithm focuses on flaw

- Flaws include texture distortion, deformation, and misalignment.

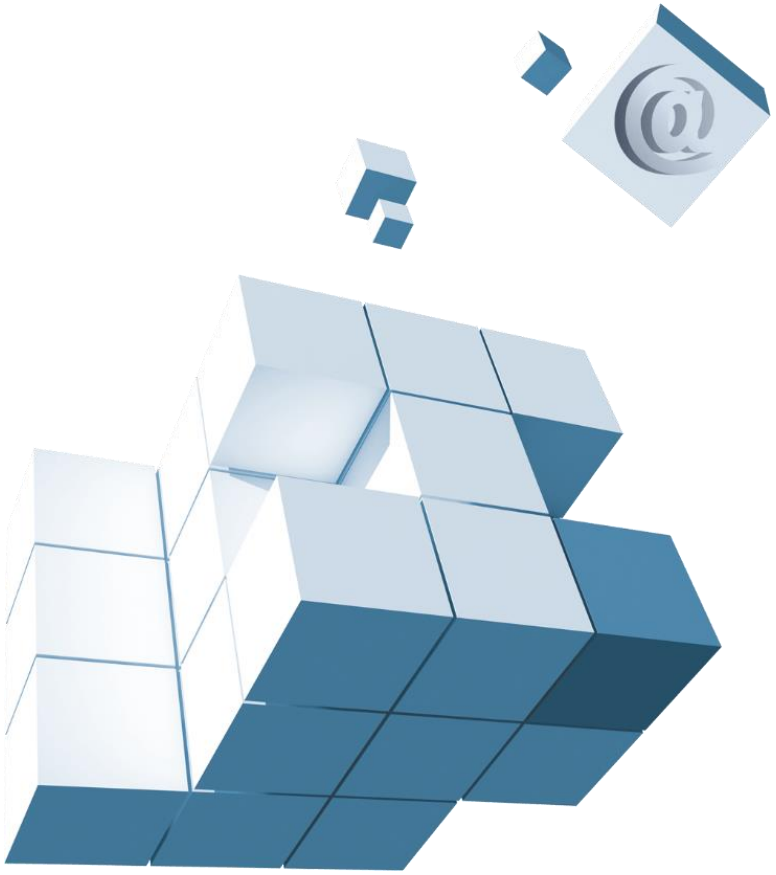
Evolutionary video interactive challenge and flaw detection architecture

- Regularly updating challenge solution.

real person authentication system

Real Person Authentication techniques safeguarding user security, ensuring user authenticity

Key Capability of Zero Trust



Supervision Hosting Service

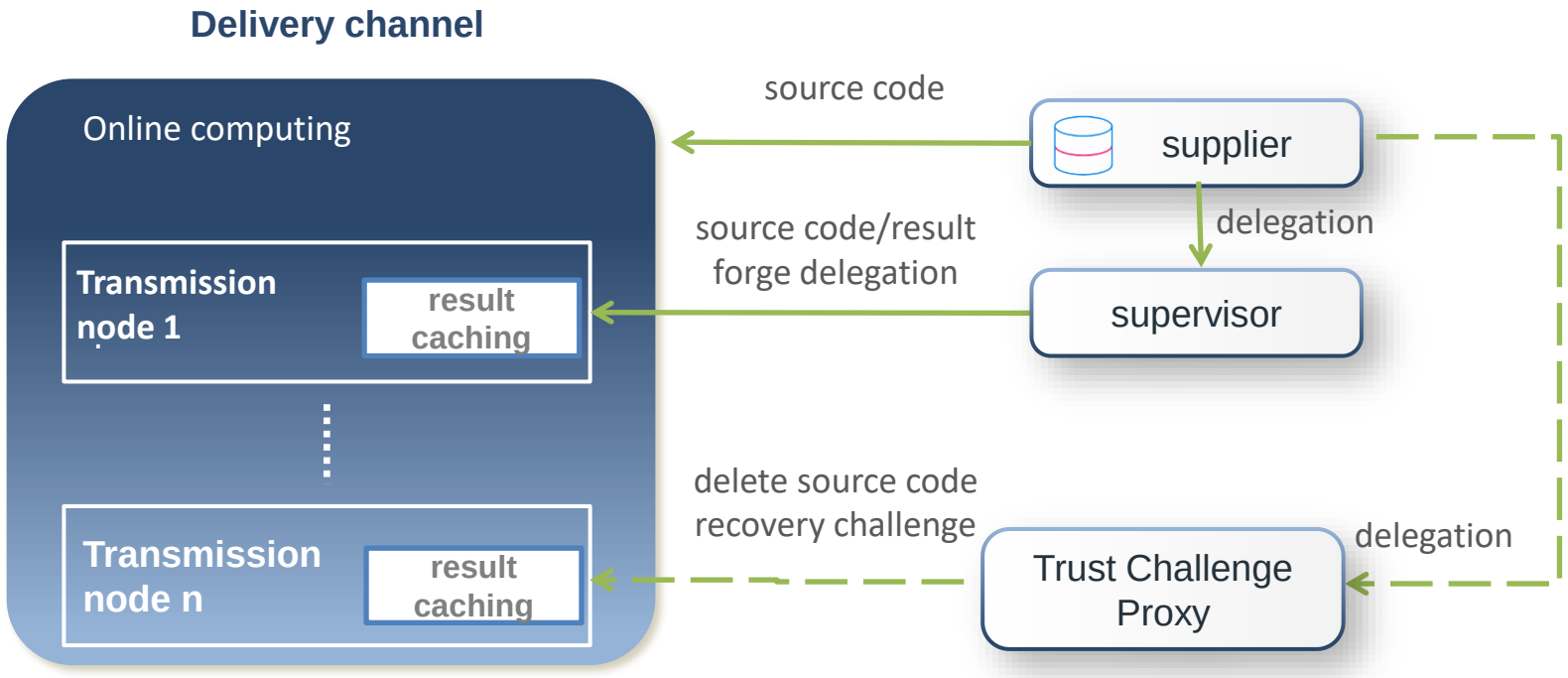
Delegating the execution of critical security policies or security tasks to an independent and authoritative third party ensures, entities that obtain temporary or managed authorization for specific resources will not pose security risks..

- **Hosted security domain**
- **Hosted audit privilege**
- **Hosted data lifecycle management**

Reference Scenario of Supervision Hosting Service

Supervised deposit agreement: delete within the specified time after online computing

Supervisor: enforce physical deletion of source code in the transmission node



Report completed

Thank you for listenning !