

Security Considerations for Computing-Aware Traffic Steering

[draft-wang-cats-security-considerations-02](#)

Cuicui Wang(China Unicom) Yu Fu(China Unicom)

Security Considerations for Computing-Aware Traffic Steering

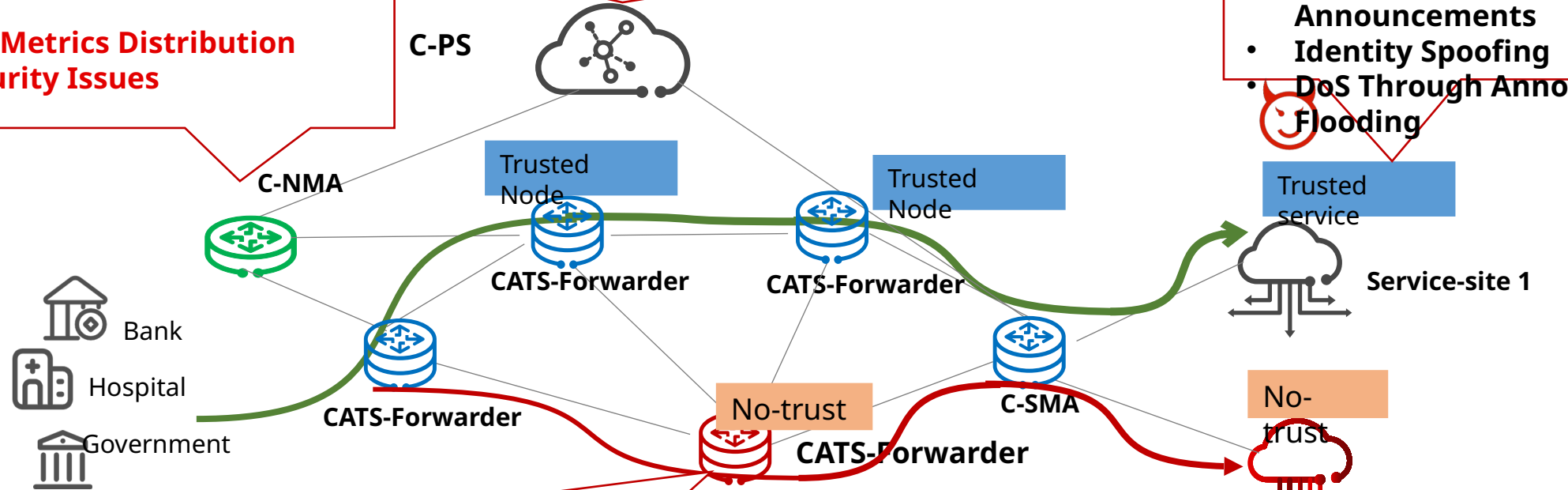


- 2、 Computing Path Selector Security Issues**
- Path Manipulation Attacks
 - Covert Channel Exploitation
 - Topology Poisoning
 - Decision Logic Corruption
 - Orchestrator Impersonation

- 3、 Computing Service Announcement Security Issues**
- Unauthorized Announcement Injection
 - Data Confidentiality Breaches
 - Replay/Reuse of Legacy Announcements
 - Identity Spoofing
 - DoS Through Announcement Flooding



- 5、 Metrics Distribution Security Issues**



- 4、 Metrics Distribution Security Issues**
- Tampering with Metric Data
 - Eavesdropping on Sensitive Metrics
 - Forged Metric Sources
 - Privacy Violation



- 1、 Security Issues of The Computing Resources**
- Unauthorized Access and Control
 - Data Confidentiality Breaches
 - Denial of Service (DoS) Threats

Security Issues of The Computing Resources

- The ubiquitous and flexible characteristics of computing resources and the frequent connections to the computing resources will lead to the following risks:

RISKS

- **Unauthorized Access and Control**

Attackers MAY exploit vulnerabilities in interfaces or APIs to gain unauthorized access, potentially **hijacking computational resources** or manipulating task execution.

- **Data Confidentiality Breaches**

Sensitive data processed by computing resources COULD be intercepted during transmission or compromised through insecure memory handling.

- **Denial-of-Service (DoS) Threats**

Malicious actors MAY flood computing resources with forged computation requests, degrading service availability or disrupting task scheduling.

COUNTERMEASURES

- **Granular Access Control**

Role-based access policies (RBAC) aligned with AAA architecture could be used to manage the data processing in computing resources. Hardware-rooted attestation could be used for runtime authorization decisions.

- **Secure Communication Frameworks**

TLS 1.3 could be adopted for all control-plane and data-plane communications. Certificate-based mutual authentication could be implemented using IETF SUIT for Computing Service to C-SMA interactions.

- **Resilience Against DoS & Continuous Monitoring**

Proof-of-work challenges for request authentication could be deployed as the resilience against DoS during traffic anomalies. Geo-distributed traffic scrubbing could be enabled through collaboration with CDN providers. Nodes could be instrumented with runtime integrity verification using OpenTelemetry standards. Anomaly detection systems

Computing Path Selector Security

Issues

- The Computing Path Selector which is responsible for dynamically selecting optimal forwarding paths, faces the following threats:

POTENTIAL RISKS

- Path Manipulation Attacks**

Adversaries may forge or alter path metadata to steer computation tasks toward compromised nodes.

- Covert Channel Exploitation**

Path selection patterns could be abused to leak sensitive information through timing analysis or topology fingerprinting.

- Topology Poisoning**

Injection of forged network topology data could degrade path selection efficiency or enable man-in-the-middle (MITM) attacks.

- Decision Logic Corruption**

Runtime modification of C-PS algorithms may lead to suboptimal or adversarial path selections.

- Orchestrator Impersonation**

Spooled control-plane messages could trick CPS into accepting unauthorized path directives.

COUNTERMESURES

- Authenticated Path Metadata**

Digitally sign topology updates and node capability information could be implemented using CBOR Object Signing and Encryption. Enforce strict schema validation for path

- Decision Integrity Protection**

C-PS path selection logic could be isolated in hardware-rooted trusted execution environments (TEEs). Runtime attestation of decision engines could be implemented via Remote Attestation

- Differential Privacy for Path Selection**

Sensitive selection patterns could be Obfuscated by incorporating differentially private noise.

- Resilient Topology Discovery**

RPKI or BGPsec principles could be adopted for secure topology propagation in multi-domain scenarios.

- Control-Plane Hardening**

Mutual authentication could be adopted in communications between C-PS and C-SMA or C-NMA via OAuth 2.1.

Computing Service Announcement Security Issues

- The announcement of computing services in distributed environments introduces several security risks that must be addressed to ensure system integrity, confidentiality, and availability. This section outlines key threats and proposed countermeasures.

POTENTIAL RISKS

- **Unauthorized Announcement Injection**
Malicious actors may forge or manipulate service announcements to advertise rogue computing nodes, redirect traffic to compromised resources, or disrupt service discovery, which may lead to data exfiltration, computation tampering, or denial of service.
- **Sensitive Information Exposure**
Unauthorized interception of metrics may cause the eavesdropping on sensitive operational details, which will lead to the exposure of business-critical intelligence or user behavior profiling.
- **Replay/Reuse of Legacy Announcements**
Replayed announcements of deprecated services could lead to resource misallocation or dependency on outdated/insecure compute nodes.
- **Identity Spoofing**
Impersonation of legitimate service providers through forged identity claims in announcements.
- **DoS Through Announcement Flooding**
Flooding the control plane with excessive or malformed announcements may lead to system resources exhausted.

COUNTERMEASURES

- **Cryptographic Integrity Protection**
Digital signatures (e.g., using COSE/JOSE) could be adopted for all announcements to ensure authenticity and integrity. Verifiable attestation (via frameworks like RATS) could be used for critical service claims.
- **Metadata Minimization & Encryption**
Data minimization principles could be applied to limit exposed metadata in announcements. Hybrid encryption (e.g., ECIES) could be used for sensitive fields while maintaining routable/public attributes in cleartext.
- **Anti-Replay Mechanisms**
Timestamp/nonce could be used in announcements with strict freshness validation.
- **Rate Limiting & Prioritization**
QoS controls could be applied to prioritize announcements from authenticated entities. Rate limits per node/domain could be adopted using token-bucket or similar algorithms.
- **Identity Verification**
The announcement from the computing devices could be binded to DIDs (Decentralized Identifiers) or VCs (Verifiable Credentials) for cryptographic identity proof.

Metrics Distribution Security Issues

- Metrics distribution mechanisms in CATS are critical for performance optimization and resource coordination. However, they introduce specific security challenges that must be mitigated to prevent misuse or systemic compromise. This section identifies key threats and proposes

POTENTIAL RISKS

- **Tampering with Metric Data**

Adversaries may alter metrics (e.g., latency, throughput, resource utilization) during transmission to mislead the decision-making of control plane, triggering suboptimal traffic placement or resource allocation and leading to degraded service performance.

- **Eavesdropping on Sensitive Metrics**

Unauthorized interception of metrics may cause the eavesdropping on sensitive operational details (e.g., geo-location patterns, infrastructure capacity), which will lead to the exposure of business-critical intelligence or user behavior profiling.

- **Forged Metric Sources**

Spoofing of metric publishers to inject false data or impersonate trusted entities (e.g., fake "low-load" signals to attract traffic).

- **Privacy Violations via Aggregation**

The statistical analysis of aggregated metrics may produce inference of sensitive information (e.g., user activity, infrastructure weaknesses) which may result in privacy violation.

COUNTERMEASURES

- **End-to-End Integrity Protection**

Cryptographic signatures (e.g., using COSE/JOSE) could be applied to metric payloads to ensure authenticity and detect tampering. Hash-chaining or Merkle trees could be used for batch metric verification in streaming scenarios.

- **Confidentiality Preservation**

Sensitive metric fields could be encrypted (e.g., using AES-GCM or HPKE) while preserving routable headers in plaintext. Differential privacy or noise injection could be employed for aggregated metrics to prevent inference attacks.

- **Source Authentication**

Metric publishers could be bound to cryptographically verifiable identities (e.g., X.509 certificates, DIDs). Role-based access control (RBAC) could be used for metric publication rights.

- **Privacy-Aware Metric Design**

The high-granularity data (e.g., masking exact geolocation to regional levels) could be anonymized or truncated to protect the privacy. The federated learning or on-device aggregation could be used to minimize raw data exposure.

Security-related Metrics

- The service and network metrics could include the security-related capabilities which could be used by the CATS Path selector to compute paths with security guarantee.
- The security capabilities of nodes could be one of the metrics for C-PS to computing the traffic forwarding path and form a secure routing path. And C-PS will fetch the real-time awareness of the security capabilities available in the network and computing services and finally provide security protection for users. Clients with high security requirements could choose the service with desired security attributes and achieve dependable forwarding on top of only devices that satisfies certain trust requirements, which will avoid the risks of traffic eavesdropping, sensitive data leakage etc.

Welcome Comments

- Welcome sharing your insights on enhancing the security aspects of CATS
 - Any suggestions on the security analysis and measures outlined in the draft ?
 - if the document covers all critical aspects of CATS security or if additional measures should be addressed.

Thanks !