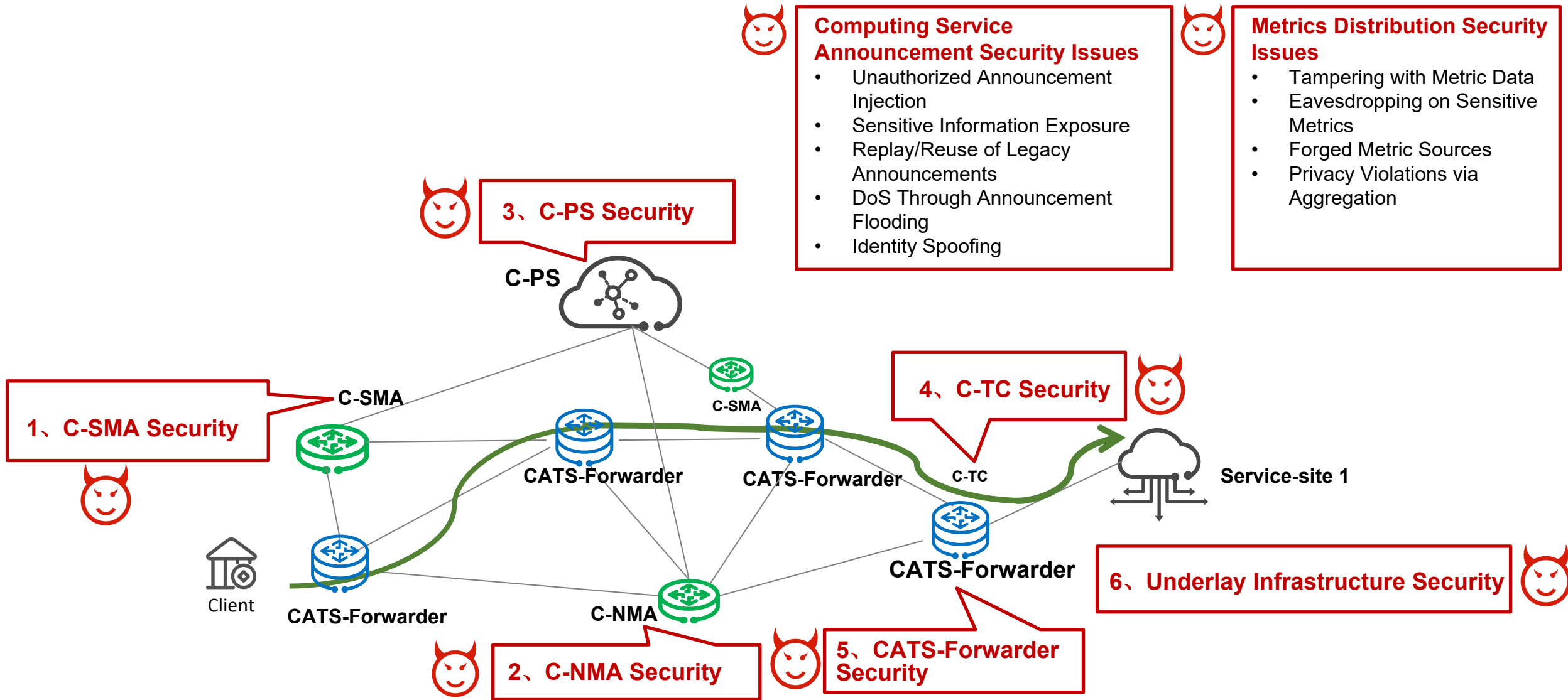


Security Considerations for Computing-Aware Traffic Steering

[draft-wang-cats-security-considerations-04](#)

Jinyu Shi, Cuicui Wang, Yu Fu
China Unicom

Security Considerations for Computing-Aware Traffic Steering



Security Issues of CATS Service Metric Agent (C-SMA)

The CATS Service Metric Agent (C-SMA), which is responsible for collecting service capabilities and status, faces the following threats:

POTENTIAL RISKS

Man-in-the-Middle (MITM) Attack

Attackers may forge nodes or hijack links to report false metrics (e.g., resource utilization), leading to incorrect path decisions.

False Service Instance Registration

Attackers can register fake instances without strict authentication, causing C-SMA to collect and distribute invalid metrics.

Denial of Service (DoS) Attack

Attackers send a large number of requests to exhaust computing resources, making it unable to collect legitimate metrics.

COUNTERMEASURES

Deploy C-SMA in a Trusted Zone

Place C-SMA inside the service site or trusted area of the egress Forwarder, restrict direct external access via firewalls.

Enforce Rate Limiting for Requests

Set a threshold for single-source collection requests to block malicious flood requests and avoid Denial of Service attacks.

Whitelist Mechanism for Service Instances

Only collect metrics from whitelisted instances. Enforce strict identity authentication (e.g., digital certificates) for new registrations.

Security Issues of CATS Network Metric Agent (C-NMA)

The CATS Network Metric Agent (C-NMA), which collects sensitive network data, is vulnerable to the following risks:

POTENTIAL RISKS

Sniffing Attack

Sensitive network data (latency, topology) may be intercepted, enabling attackers to identify weak nodes.

False Metric Injection

Vulnerabilities in reused protocols (OSPF/IS-IS) may allow injection of fake metrics, distorting network perception.

Protocol Vulnerability Exploitation

Unpatched vulnerabilities in running protocols can be exploited to infiltrate the CATS network.

COUNTERMEASURES

Adopt security-enhanced routing protocols

Use OSPFv3 (AES-128) or IS-IS (HMAC-SHA256) for secure metric collection and transmission, preventing fake metric injection.

Implement data desensitization

Distribute only core decision-making metrics (e.g., normalized latency) to C-PS, masking sensitive topology details (e.g., non-critical IPs) to avoid leakage.

Regularly update NMA firmware/protocols

Patch vulnerabilities per IETF RFC standards and conduct quarterly security scans.

Encrypt transmission links

Use TLS 1.3 (RFC8446) with mutual certificate authentication between C-NMA and C-PS to prevent MITM attacks.

Security Issues of CATS Traffic Classifier (C-TC)

The CATS Traffic Classifier (C-TC), which classifies service traffic, is exposed to the following security risks:

POTENTIAL RISKS

Classification Rule Tampering

Attackers may tamper with the rule table to disguise malicious traffic as legitimate service traffic, bypassing checks to enter the CATS network.

Fake Classification Result Forgery

Without authentication on the collaboration link, attackers can forge results, leading to incorrect discarding or forwarding of legitimate traffic.

COUNTERMEASURES

Encrypt and Incremental Updates

Store rules in AES-256 encrypted form and implement incremental updates with multi-factor authentication to prevent unauthorized modification.

Active-Standby C-TC Cross-Validation

Deploy primary and backup C-TCs on the ingress Forwarder; forward traffic only when both outputs are consistent, avoiding single-point hijacking errors.

Log classification operations in real time

Record all classification rule changes and traffic classification results in an immutable audit log (append-only mode) to facilitate traceability in case of security incidents.

Validate CS-ID/CSCI-ID legitimacy

Deploy primary and backup C-TCs on the ingress Forwarder; forward traffic only when both outputs are consistent, avoiding single-point hijacking errors.

Security Issues of CATS-Forwarders

CATS-Forwarders, which forward traffic to service instances, encounter the following security challenges:

POTENTIAL RISKS

Encryption Key Leakage

Stolen keys enable decryption of overlay traffic and theft of service requests

Fake Service Instance Forwarding

Traffic is forwarded to unverified fake instances, leading to hijacking.

Flood Traffic Attack

Malicious requests consume bandwidth and computing resources.

COUNTERMEASURES

Regular Key Rotation

Use AES-256-GCM, rotate keys automatically (e.g., every 7 days), and store in HSMs.

CSCI-ID & Certificate Binding

Verify digital certificates of Service Contact Instances before forwarding.

Traffic Cleaning

Integrate DDoS protection to filter malicious flood traffic and non-compliant protocols.

Overlay/Underlay Isolation

Use VXLAN with MACsec to isolate CATS traffic from the underlying network.

Security Issues of CATS Path Selector (C-PS) (No Updates)

The Computing Path Selector (C-PS), 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 (e.g., node capabilities, network latency) 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.

COUNTERMEASURES

Authenticated Path Metadata

Digitally sign updates using COSE [RFC9052]. Enforce strict schema validation for path attributes per IETF YANG models [RFC7950].

Decision Integrity Protection

Isolate logic in hardware-rooted TEEs. Implement runtime attestation of decision engines via Remote Attestation Procedures (RATS) [RFC9334].

Differential Privacy for Path Selection

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

Security Issues of Underlay Infrastructure (No Updates)

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

POTENTIAL 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 (e.g., model parameters) could be intercepted during transmission or compromised through insecure memory handling.

Denial-of-Service (DoS) Threats

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

COUNTERMEASURES

Granular Access Control

Use RBAC aligned with AAA architecture and hardware-rooted attestation (e.g., TPM) for runtime authorization decisions.

Secure Communication Frameworks

Adopt TLS 1.3 for all communications and implement certificate-based mutual authentication using IETF SUIF for secure interactions.

Resilience Against DoS

Deploy proof-of-work challenges for request authentication and enable geo-distributed traffic scrubbing via CDN collaboration.

Continuous Monitoring

Instrument nodes with runtime integrity verification via OpenTelemetry and establish federated learning-based anomaly detection to identify cross-node attack patterns.

Security Issues of Service Announcement (No Updates)

The Service Announcement workflow faces the following security issues and corresponding countermeasures:

POTENTIAL RISKS

Unauthorized Announcement Injection

Sensitive Information Exposure

Replay/Reuse of Legacy Announcements

DoS Through Announcement Flooding

Identity Spoofing

COUNTERMEASURES

Cryptographic Integrity Protection

Metadata Minimization & Encryption

Anti-Replay Mechanisms

Rate Limiting & Prioritization

Identity Verification

Security Issues of Metrics Distribution (No Updates)

The Metrics Distribution workflow faces the following security issues and corresponding countermeasures:

POTENTIAL RISKS

Tampering with Metric Data

Eavesdropping on Sensitive Metrics

Forged Metric Sources

Privacy Violations via Aggregation

COUNTERMEASURES

End-to-End Integrity Protection

Confidentiality Preservation

Source Authentication

Privacy-Aware Metric Design

Thanks !