TRACE-5G: Trust-Aware Runtime Attestation and Continuous Enforcement for 5G User Equipment

Al Nahian Bin Emran*, Rajendra Paudyal*, Rajendra Upadhyay*, Arupjyoti Bhuyan†, Duminda Wijesekera*
*Mason Innovation Labs, George Mason University, 3434 Washington Blvd Suite 1300, Arlington, VA, USA
†Idaho National Laboratory, 1955 Fremont Ave, Idaho Falls, ID 83415, USA
{abinemra, rpaudyal, rupadhya, dwijesek}@gmu.edu, arupjyoti.bhuyan@inl.gov

***Abstract*—The standard 5G Authentication and Key Agreement protocol (5G-AKA) authenticates subscriber credentials but does not verify the integrity of user equipment (UE). Existing literature includes admission-time device-certificate authentication and Trusted Platform Module (TPM)-based measured-boot attestation, which can additionally verify that the UE presents enrolled device credentials and boots into an approved state. However, these checks do not reveal whether harmful unauthorized software is executed after admission. We present TRACE-5G, which continuously verifies the UE's runtime software state and uses the resulting trust state to control network access. TRACE-5G retains the pre-admission certificate and boot checks, and in addition places the admitted UE in restricted connectivity while runtime integrity is verified. Linux Integrity Measurement Architecture (IMA) records runtime software measurements, TPM PCR (Platform Configuration Register) cryptographically accumulates them, and Keylime, a remote-attestation framework, repeatedly evaluates TPM and IMA evidence against enrolled references. A Trusted result grants full access on the existing PDU session, but an Untrusted result withholds or removes full access and causes network deregistration. We implement TRACE-5G on an srsRAN/Open5GS testbed with a hardware TPM2.0 UE and core-side firewall enforcement. Across ten trusted trials, Level 2 access was established in 9–12s. Across ten untrusted trials, promotion was consistently withheld; in a representative trace, restrictive policy was applied within 5ms of the Untrusted decision and UE-context release completed within 1.670s. TRACE-5G extends UE trust beyond admission without any modification of the standardized 5G protocols.**

***Index Terms*—5G security, remote attestation, Trusted Platform Module 2.0, IMA, Keylime, runtime integrity, UE, Zero Trust**

I. Introduction

The 5G security architecture uses 5G Authentication and Key Agreement protocol (5G-AKA) to authenticate a subscriber and derive keys that protect Non-Access Stratum (NAS) and Access Stratum signaling [1]. However, subscriber authentication does not establish that the physical user equipment (UE) remains trustworthy. Examples that violate would a valid USIM may be used in an unauthorized platform, a legitimate UE may boot from modified software, or an admitted UE may later execute unauthorized software. Admission-time device attestation addresses part of this problem. Battlefield 5G adds two independent device-certificate checks and Trusted Platform Module (TPM)-based Platform Configuration Register (PCR) 0–7 boot attestation before normal 5G registration [2]. These checks bind network admission to an enrolled device and approved boot state, but the resulting trust decision remains point-in-time because PCRs 0–7 do not describe software changes that occur after admission. Consequently, a UE that later executes unauthorized software may continue to retain network access because its runtime integrity is not re-evaluated.

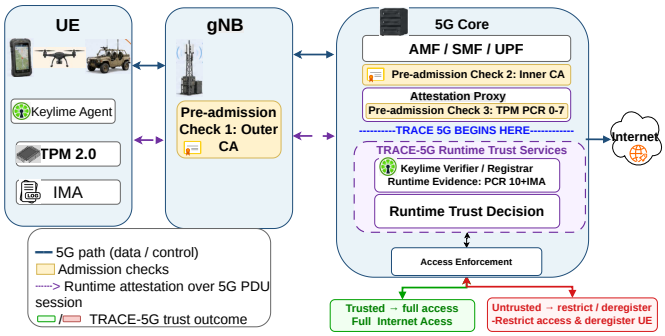

Fig. 1. TRACE-5G UE Trust and Enforcement Architecture

Continuous attestation provides a way to evaluate integrity after this initial decision. A TPM provides a hardware-backed root of trust and protects attestation keys and measured state, while the Linux Integrity Measurement Architecture (IMA) measures runtime files and executables [3]. Separately, Keylime is a remote-attestation framework that repeatedly evaluates TPM and IMA evidence to maintain an updated integrity state [4]. Emran et al. applied TPM, IMA, and Keylime with container-aware measurement attribution to Kubernetes-hosted 5G core functions [5]. That work attests 5G infrastructure, whereas TRACE-5G addresses the continued authorization of an active cellular UE whose runtime state can change after admission. Consequently, TRACE-5G treats network authorization as a continuously re-evaluated decision, $\mathcal{A}_{UE}(t) = f(I_{dev}, I_{boot}, I_{runtime}(t))$, where I_{dev}, I_{boot}, and $I_{runtime}(t)$ represent the enrolled device identity, boot integrity, and runtime integrity at time t. A UE first satisfies the device and boot checks, enters restricted connectivity, and receives full access only after its runtime state is verified. Continued full access remains conditional on subsequent runtime attestation. This approach aligns with Zero Trust Architecture (ZTA) principles by making continued network access conditional on current device posture rather than treating successful admission as permanent trust [6].

Figure 1 shows the TRACE-5G architecture. The three pre-admission checks remain at their existing enforcement points:

Outer CA verification at the gNB, independent Inner CA verification at the AMF, and TPM PCR 0–7 boot-attestation verification through the core-side attestation proxy [2]. After these checks succeed, standard 5G-AKA and registration proceed and the UE establishes a restricted PDU session. TRACE-5G then evaluates PCR 10 and container-aware IMA runtime evidence over the UE–gNB–core 5G path. A Trusted result grants full network access to the existing session, whereas an Untrusted result prevents or withdraws full-access authorization and triggers network-requested deregistration. The contributions of this work are as follows.

- We introduce a staged UE trust lifecycle that separates admission-time trust from runtime trust. After passing device-identity and boot-integrity checks, the UE remains restricted until its runtime software state is verified using TPM PCR 10 and IMA measurements. Full network access remains conditional on continued runtime trust verification.
- We connect the resulting Keylime trust state to 5G network access. A Trusted UE receives full access on its existing PDU session, while an Untrusted UE remains or becomes restricted and is subsequently deregistered. No Data Network Name (DNN) change, address reassignment, or PDU-session re-establishment is required.
- We implement TRACE-5G on a hardware-TPM srsRAN/Open5GS testbed without introducing new standardized NAS/RRC message types. Across ten trusted trials, runtime trust and Level 2 access were established in approximately 9–12 s. Across ten untrusted trials, the same enforcement sequence was observed; in a representative trace, the restrictive policy followed the Untrusted decision within 5 ms and UE-context release is completed within 1.670 s.

II. Background and Related Work

A. 5G-AKA and the Device-Trust Gap

The 5G Authentication and Key Agreement (5G-AKA) protocol authenticates a subscriber and establishes the key hierarchy used to protect Non-Access Stratum (NAS) signaling between the UE and AMF and the Access Stratum signaling between the UE and gNB [1]. The procedure primarily authenticates the subscriber credential anchored in the USIM rather than the integrity of the physical platform hosting that credential. Formal analyses of 5G authentication similarly focus on subscriber authentication, key agreement, unlinkability, and privacy, rather than the runtime software state of the UE [7]. Consequently, successful 5G-AKA does not by itself establish that the UE is an enrolled device, that it booted into an approved software state, or that its software remains trustworthy after authentication.

Prior cellular-security research has strengthened connection bootstrapping and base-station authentication. Hussain et al. showed that weaknesses during cellular bootstrapping can enable multiple attacks [8], while Singla et al. and other work proposed stronger mechanisms for secure 5G bootstrapping and base-station authentication [9]–[11]. These approaches improve the establishment of a secure cellular connection but they do not continuously evaluate the integrity of an already-connected UE. Emran et al. proposed Battlefield 5G to address the complementary pre-admission device-trust problem [2]. Their work introduces three checks performed before normal registration proceeds: (1) an Outer CA certificate verification at the gNB, (2) an independent Inner CA verification at the AMF, and (3) TPM-based boot attestation using PCRs 0–7. These checks allow a credential-validation, but unauthorized or boot-tampered devices to be rejected before admission. However, the resulting trust decision is established only at connection time; The boot evidence from PCR 0–7 does not describe software changes that occur later during the active UE session.

B. TPM, IMA, and Remote Attestation

A Trusted Platform Module (TPM) is a hardware security component that provides protected cryptographic operations, key storage, and Platform Configuration Registers (PCRs) that support hardware-rooted integrity measurement [12]. During measured boot, measurements of firmware, bootloader, kernel, and other component of the platform are cumulatively extended to selected PCRs. Then an Attestation Key (AK) can sign a fresh TPM quote over those PCR values and a verifier-provided nonce, allowing a remote verifier to check both platform state and evidence freshness.

Linux Integrity Measurement Architecture (IMA) extends integrity measurement to runtime software. IMA records measurements of files and executables according to a configured policy and extends their digests into PCR 10. During remote attestation, the verifier checks the AK-signed quote and nonce, verifies that the IMA measurement history is consistent with the quoted PCR 10 value, and compares measured objects with configured reference values or allow-lists. This follows the general Internet Engineering Task Force (IETF) Remote ATtestation ProcedureS (RATS) model, in which an attester provides evidence that a verifier evaluates against trusted reference values to produce an attestation result [13].

C. Keylime Framework

Keylime is an open-source framework for TPM and IMA-based remote attestation [4]. A Registrar maintains TPM identity information, an Agent on the attested platform provides TPM and IMA evidence, and a Verifier repeatedly evaluates that evidence to maintain an updated trust state. Operational studies have demonstrated Keylime's ability to detect measured runtime integrity violations while also highlighting practical issues such as allow-list maintenance and measurement coverage [14]. Emran et al. applied Keylime with container-aware IMA attribution to continuously attest Kubernetes-hosted 5G core functions [5]. In that work, the attested subjects were 5G Core components. Instead TRACE-5G attests an active UE and connects its runtime trust state to continued network authorization. Table I summarizes the difference between standard 5G-AKA, Battlefield 5G, and

TABLE I
POSITIONING OF TRACE-5G IN THE UE TRUST LIFECYCLE

Approach	UE Trust Checks	UE Lifecycle Coverage	Access / Enforcement Outcome
5G-AKA [1]	Subscriber authentication using USIM credentials	Authentication	Authenticates the subscriber and establishes security keys
Battlefield 5G [2]	Check 1: Outer certificate at the gNB; Check 2: Inner certificate at the AMF; Check 3: TPM PCR 0–7 boot attestation verified by the core attestation proxy	Pre-admission only	Admits UE if all three checks succeed; else reject
TRACE-5G	**Perform Checks 1–3 for pre-admission assurance; Add continuous post-admission UE runtime attestation using TPM PCR 10 and container-aware IMA measurements, verified by the core-side Keylime Verifier**	**Pre-admission checks followed by continuous post-admission runtime verification**	**Post-admission, keeps the UE in restricted access until runtime trust is established; then grants full access. If runtime trust is lost, revoke access deregister the UE**

TRACE-5G in terms of the coverage of UE trust and the enforcement of the network.

III. THREAT MODEL AND DESIGN GOALS

We consider a private/tactical 5G deployment where the operator controls the gNB, core, Keylime services, enrollment infrastructure, and TPM trust anchors. An adversary may transplant a valid SIM, use an unauthorized device, modify boot components, introduce unauthorized runtime software/containers, modify measured executable content, or replay captured evidence. We assume that the attacker cannot extract TPM-resident keys, forge trusted-CA signatures or fresh TPM quotes, or subvert the trusted kernel/IMA path. RF denial-of-service, TPM compromise, and attacks outside the configured IMA measurement coverage are beyond the scope. Our design goals are: *G1* verify enrolled identity and boot state before admission; *G2* bootstrap attestation with restricted connectivity; *G3* repeatedly verify runtime integrity; *G4* translate trust loss into data- and control-plane enforcement; and *G5* preserve standardized NAS/RRC message formats.

IV. TRACE-5G SYSTEM DESIGN

TRACE-5G organizes UE trust into three levels. *Level 0* represents pre-admission device and boot assurance with no network access; *Level 1* provides restricted connectivity while runtime trust is established; and *Level 2* provides full connectivity conditioned on continuous attestation. An untrusted verdict prevents promotion to Level 2 or withdraws existing Level 2 authorization and returns the UE to Level 0 by deregistration. Figure 2 summarizes this lifecycle. TRACE-5G also preserves the standard 5G control-plane procedures. After the Checks 1–3 are successful, normal 5G-AKA and registration are executed, and Level 1 connectivity is established through the standard establishment of the PDU session. Promotion to Level 2 is only a core-side policy update on the existing session, while trust loss uses standard network-requested deregistration and UE-context release. No new NAS or RRC message types or message formats are introduced.

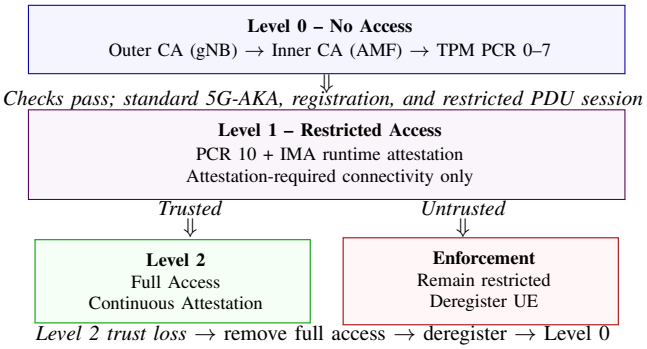

Fig. 2. TRACE-5G UE trust lifecycle.

A. One-Time Enrollment

Before deployment, the UE is enrolled in a trusted environment. The activation of the TPM endorsement key (EK) and the attestation key (AK) binds the AK to the intended hardware TPM, while PCR 0–7 from a known-good boot establish the boot reference values and PCR 10 is included in the runtime-attestation policy. The operator generates host and per-container allow-lists, and TRACE-5G uses the `ima-dep-cgn` [15] template with the `cgpath` field to identify whether each measurement belongs to the host or a specific container. The UE's Keylime Agent is registered with the attestation infrastructure and associated with a persistent Keylime identity. A core-side enrollment database stores the EK/AK metadata, PCR policy, Keylime identity, runtime reference information, and session-association metadata required for subsequent admission and runtime verification. These trusted values and allow-lists remain at the core and are not supplied by the fielded UE during attestation.

B. Level 0: Admission-Time Assurance

TRACE-5G uses as its Level 0 foundation the three-stage pre-authentication design introduced by [2]. After RRC establishment, the gNB performs Check 1 by challenging the UE and validating its Outer CA device certificate and nonce signature before forwarding the Registration Request. At AMF, Check 2 independently validates the Inner CA certificate and a fresh nonce signature. Check 3 then challenges the hardware TPM for an AK-signed quote over PCRs 0–7; the core-side attestation proxy verifies the AK, quote signature, freshness, and PCR values against the enrolled boot baseline. The Registration Request is preserved while these checks execute and enters normal processing only after all three succeed. Then the standard 5G-AKA and registration proceed. Checks 1–3 establish device identity and boot integrity at admission time, but do not describe the subsequent runtime software state; TRACE-5G therefore places the admitted UE into Level 1 rather than granting unrestricted access immediately.

C. Level 1: Restricted Access

After Level 0 succeeds, TRACE-5G initializes runtime monitoring and allows standard 5G registration to complete. The UE then establishes a PDU session through a dedicated restricted DNN using the standard PDU Session Establishment procedure. This places the UE in Level 1. The core-side access policy permits only the connectivity required for attestation and withholds normal full-access privileges until runtime trust is established. A persistent Keylime Agent runs on the UE and communicates with the core-side attestation infrastructure through this restricted 5G PDU session. Thus, runtime attestation is performed over the same radio-connected data path whose access is being evaluated.

For each attestation cycle, the Agent provides a fresh TPM quote over PCR 10 together with the IMA measurement information. The Keylime Verifier validates the quote signature and freshness, checks that the IMA measurement history is consistent with the quoted PCR 10 value, and compares the measured hashes with the enrolled allow-lists. Using the container-aware `cgpath` field, host measurements are evaluated against the host allowlist, while container measurements are evaluated against the corresponding container-specific allow-list. The resulting verdict represents the UE's current runtime trust. An unexpected executable, unauthorized container, or measured object whose digest differs from its approved reference value can produce an untrusted verdict. In that case, Level 2 promotion is withheld, the restricted policy remains active, and the UE proceeds towards deregistration. Only a UE whose runtime measurements satisfy the configured policy advances to Level 2. TRACE-5G therefore separates successful network admission from authorization for full network use.

D. Level 2: Full Access with Continuous Monitoring

When the Keylime Verifier reports that the UE is trusted, TRACE-5G promotes the UE from restricted connectivity at Level 1 to full access at Level 2. The attestation proxy updates the core-side access policy for the existing session without any DNN change, IP-address reassignment, or PDU-session re-establishment. Promotion does not terminate attestation. The Keylime Verifier continuously obtains fresh PCR 10 and IMA evidence and updates the runtime trust state of UE. Level 2 therefore represents full access conditioned on continued compliance with the configured runtime integrity policy rather than a permanent trust decision.

E. Revocation and Re-Admission

If continuous runtime attestation reports that the UE is untrusted while in Level 2, TRACE-5G removes the full-access firewall policy and reverts back to the restrictive policy for the existing session. The AMF then observes the untrusted state and initiates standard network-requested deregistration, followed by UE-context release. If the UE is still in Level 1 when it is reported as untrusted, the restrictive firewall policy is already in place. Therefore, TRACE-5G withholds the promotion of Level 2, and AMF proceeds with deregistration and release in the context of UE. After deregistration, the previous runtime-trust state is cleared. If the UE reconnects, it must restart from Level 0 and again pass Check 1, Check 2, and Check 3 before standard 5G registration proceeds and the UE can re-enter Level 1 runtime-trust establishment. Consequently, TRACE-5G connects runtime attestation directly to network authorization through *measure* → *attest* → *verify* → *authorize* → *enforce*.

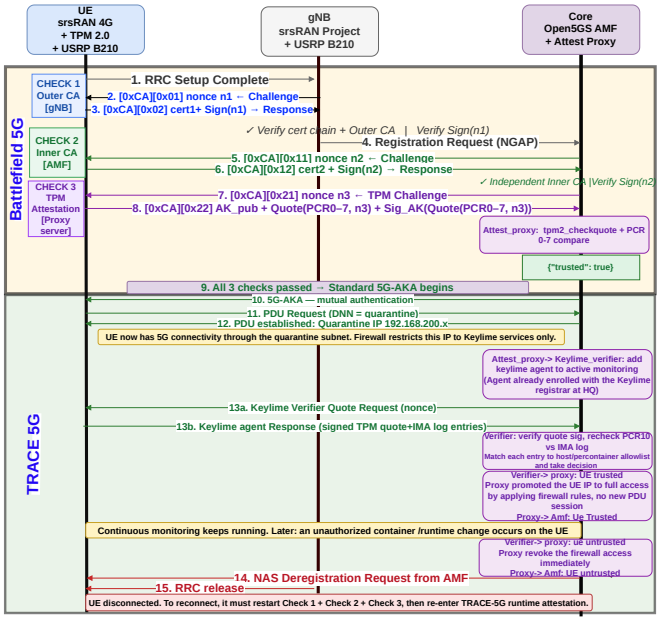

Fig. 3. End-to-end TRACE-5G communication and enforcement flow.

V. Implementation and Experimental Setup

We implemented TRACE-5G on a three-machine 5G SA testbed. The core runs Open5GS in Docker, with the Keylime Verifier and Registrar on the host and the attestation proxy in Docker. The gNB uses srsRAN Project with an Ettus USRP B210. The UE uses srsUE in 5G SA mode with an Ettus USRP B200, a Nuvoton NPCT75x hardware TPM 2.0, and a custom Linux 5.13.19 kernel containing the container-aware IMA template. Figure 3 shows the communication flow from pre-admission verification to runtime attestation and enforcement.

A. Enrollment and Pre-Admission Integration

For the prototype, the one-time enrollment described in Section IV was completed prior to the experiments. The UE's Keylime Agent was registered with the core-side Keylime Registrar, while the enrollment database and trusted reference information were maintained on the core. The enrollment record associated the UE with its TPM and Keylime identities, PCR policy, runtime reference information, and restricted-session information used during attestation and enforcement.

The pre-admission implementation retains the three-check mechanism of Battlefield 5G [2]. For Check 1, the gNB RRC path holds the UE's Registration Request while the Outer CA certificate and nonce signature are verified. The request is forwarded to the AMF through NGAP only after Check 1

succeeds. At the AMF, the Registration Request is temporarily saved while Checks 2 and 3 are executed. The Check 2 validates the independent Inner CA certificate and the nonce signature. For Check 3, the AMF forwards the UE's TPM evidence to the attestation proxy. The proxy verifies the enrolled AK, quote signature, challenge freshness, and PCR 0–7 values against the enrolled boot baseline. After Check 3 succeeds, the AMF creates the per-UE TRACE-5G runtime state and starts the runtime-monitoring process. The saved Registration Request is then returned to the normal Open5GS path, where standard 5G-AKA and registration continue. Runtime trust remains pending until the UE obtains the connectivity required for Keylime attestation.

B. Runtime Attestation and Enforcement Implementation

After registration, the UE establishes a PDU session through the dedicated restricted DNN. The Open5GS SMF/UPF provides the UE with its restricted-session address, which is associated with the corresponding UE and Keylime runtime state. The core-side firewall policy initially permits the connectivity required for runtime attestation while withholding normal full-access traffic. The UE runs a persistent Keylime Agent with the hardware TPM and the container-aware IMA kernel. Once the restricted PDU session is available, the Agent communicates with the core-side Keylime infrastructure through the UE's 5G PDU-session interface.

The UE IMA policy measures executable launches using `BPRM_CHECK` with `MAY_EXEC` and executable memory mappings using `FILE_MMAP` with `MAY_EXEC`. The container-aware IMA template includes the `cgpath` field, which identifies the execution context of each measurement. Host measurements are compared with the enrolled host allow-list, while measurements from a container are compared with the corresponding container-specific allow-list. The Keylime Verifier evaluates these IMA measurements together with fresh TPM evidence over PCR 10 and maintains the UE's runtime trusted state. The Open5GS AMF was extended with per-UE Keylime state and functions to start, poll, and stop runtime monitoring. The attestation proxy associates the UE identity, Keylime identity, and restricted-session information with the trust state reported by the Verifier. The proxy then maps that trust state to the core-side firewall policy. A trusted result grants full access to the existing PDU session without changing the DNN, UE address, or PDU session. If the UE is reported as untrusted, the restrictive firewall policy remains in place or is restored if full access had already been granted.

The Keylime Verifier performs runtime attestation every 2 seconds. The attestation proxy queries the Verifier every 3 s, while the AMF queries the proxy every 5 s. The proxy acts directly on the Verifier state when updating the firewall policy. Therefore, access enforcement does not wait for the AMF polling cycle. The AMF independently observes the untrusted state through its poll and initiates standard network-requested deregistration. Runtime-monitoring state is stopped and cleared when the UE context is released. Verification remains pending while the configured retry process is active.

TABLE II
SECURITY COVERAGE OF BATTLEFIELD 5G AND TRACE-5G

Condition	**Battlefield 5G**	**TRACE-5G**
Unauthorized UE / invalid credential	Blocked by Outer and Inner certificate checks	Same admission protection retained
Boot tampering / replay	PCR 0–7 and fresh signed evidence	Same boot and replay protection retained
Runtime software / container violation	Outside admission scope	Detected through PCR 10/IMA and enrolled allowlists
Untrusted before Level 2	No runtime trust stage	Promotion withheld; UE remains restricted and is deregistered
Trust loss after Level 2	No continuous enforcement	Full access withdrawn; restrictive policy restored; UE deregistered

Keylime runtime attestation and trust-dependent network enforcement were exercised through the UE's restricted 5G PDU-session path.

VI. EVALUATION

The evaluation focuses on the functionality introduced by TRACE-5G: post-admission runtime-trust establishment, continuous attestation over the UE's 5G PDU-session path, trust-driven access promotion, and enforcement of an untrusted runtime state. The Level 0 mechanisms are retained from Battlefield 5G and are not re-evaluated as new contributions. Emran et al. previously demonstrated rejection of SIM transplantation, invalid device credentials, boot tampering, and replay, and reported 373.4 ms of average added onboarding overhead across six trials [2]. In TRACE-5G, Checks 1–3 were exercised as part of the complete admission-to-runtime path. All runtime experiments used the attestation configuration described in Section V.

A. End-to-End Trust-Lifecycle Validation

The complete TRACE-5G path was exercised with an enrolled, policy-compliant UE. The UE first passed Checks 1–3, completed standard 5G-AKA and registration, and established the restricted PDU session. Using this restricted PDU session, the UE's Keylime Agent exchanged attestation evidence with the core-side Keylime infrastructure. The Keylime Verifier then evaluated a fresh TPM quote over PCR 10 together with the container-aware IMA measurements. When the measurements satisfied the enrolled host and container policies, the UE was reported as Trusted and the core-side access policy was updated to provide Level 2 full access. The DNN, UE address, and PDU session remained unchanged, and continuous attestation continued after promotion.

The untrusted path was also repeated ten times. A container-level allow-list violation was already present when runtime-trust establishment began. Therefore the UE passed the Level 0 identity and boot checks and completed registration, but its runtime measurements did not satisfy the enrolled policy. The trust state moved from *Pending* to *Untrusted* while the UE was still in Level 1, so full-access promotion was withheld. The restrictive firewall policy remained active, the AMF subsequently initiated network-requested deregistration, and the UE context was released. The same enforcement sequence and comparable response timing were observed across the ten repetitions. Post-Level 2 trust-loss revocation was also functionally

TABLE III
TRACE-5G RUNTIME TRUST AND ENFORCEMENT MEASUREMENTS

Measured Interval	Result	Interpretation
Runtime monitoring start → Verifier Trusted visible	∼6.3 s	Runtime trust becomes visible
Verifier Trusted visible → full-access policy activation	∼3.0 s	Proxy propagation and policy update
Level 2 full-access activation → AMF observes Trusted	∼0.7 s	Subsequent AMF observation
Level 1 runtime-trust establishment → Level 2 full-access activation	**∼9–12 s**	**Post-admission restricted-to-full-access promotion**
Untrusted decision → restrictive policy applied	5 ms	Immediate policy enforcement
Restrictive policy applied → AMF observes Untrusted	677 ms	Trust-state propagation to AMF
AMF observes Untrusted → NAS Deregistration sent	308 ms	Control-plane reaction
NAS Deregistration sent → UE-context release	680 ms	Connection teardown
Untrusted decision → UE-context release	**1.670 s**	**Post-verdict complete disconnection**

exercised by introducing an unauthorized container after full access had been granted, which caused the UE to become Untrusted and lose full access. As observed, these experiments validate the three runtime outcomes of TRACE-5G: Pending remains restricted, Trusted receives Level 2 access, and Untrusted is prevented from obtaining full network authorization. Table II summarizes the resulting security coverage.

B. Runtime Trust and Enforcement Timing

Table III summarizes the timing results for the Trusted and Untrusted cases. Across ten trusted-promotion trials, TRACE-5G reached Level 2 full-access policy activation approximately 9–12s after runtime monitoring began. This value represents the complete runtime-trust establishment interval rather than the processing time of a single TPM quote or the delay of the firewall action itself. In a representative trace, approximately 6.3s elapsed before the Verifier exposed the Trusted state. This period includes the initial Keylime runtime verification and the asynchronous attestation process. After the Trusted state became available, full-access policy activation followed approximately 3s later, which is consistent with the proxy's 3s Verifier-polling interval. Thus, most of the observed 9–12 s delay is associated with establishing and propagating the initial runtime-trust result, while the subsequent authorization change requires approximately one proxy polling cycle.

In the untrusted experiments, an additional container not covered by the enrolled container allow-lists was deployed on the UE before runtime attestation began. When Keylime evaluated the UE's PCR 10 and IMA evidence, measurements from this container caused the UE to be reported as Untrusted. Once the Untrusted verdict became available, the restrictive firewall policy was applied within 5 ms. The AMF observed the Untrusted state 677ms after the policy action and issued the network-requested NAS Deregistration Request after a further 308ms. UE-context release completed 680ms later, giving 1.670s from the Untrusted decision to complete UE-context release. Because the additional container was deployed before runtime attestation began, these measurements do not represent container-deployment-to-detection latency. These measurements show that initial runtime-trust establishment requires several seconds, while post-verdict enforcement occurs much faster.

VII. CONCLUSION

TRACE-5G extends the trust of UE beyond admission by combining device and boot assurance with continuous runtime attestation and trust-driven network enforcement. The prototype keeps an admitted UE restricted until its runtime state is verified, then grants full access only while that trust is maintained. Across ten trusted trials, Level 2 access was established in approximately 9–12 s, representing the time required to establish runtime assurance before unrestricted access. This is a security–latency tradeoff for tactical and private 5G environments, where verifying the current integrity of the UE can be more important than granting immediate full access. Once an Untrusted decision is available, restrictive policy is applied within 5 ms in a representative trace and UE-context release completes within 1.670 s. TRACE-5G provides this protection while preserving standard 5G registration, PDU-session, and deregistration procedures.

REFERENCES

[1] "5g; security architecture and procedures for 5g system (3gpp ts 33.501 release 18)," ETSI / 3GPP, Tech. Rep., 2024.

[2] A. N. B. Emran et al., "Battlefield 5g: Dual-pki and tpm-based ue attestation for tactical 5g standalone networks," *arXiv preprint arXiv:2608.11293*, 2026.

[3] D. G. Berbecaru, S. Sisinni, A. Lioy, B. Rat, D. Margaria, and A. Vesco, "Mitigating software integrity attacks with trusted computing in a time distribution network," *IEEE Access*, vol. 11, pp. 50 510–50 527, 2023.

[4] N. Schear et al., "Bootstrapping and maintaining trust in the cloud," in *Proceedings of the 32nd Annual Conference on Computer Security Applications*, 2016, pp. 65–77.

[5] A. N. B. Emran et al., "Tpm-based continuous remote attestation and integrity verification for 5g vnfs on kubernetes," in *2025 IEEE 7th International Conference on Trust, Privacy and Security in Intelligent Systems, and Applications (TPS-ISA)*, 2025, pp. 435–444.

[6] R. Freter, "Department of defense (dod) zero trust reference architecture," 2022.

[7] D. Basin et al., "A formal analysis of 5g authentication," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, 2018, pp. 1383–1396.

[8] S. R. Hussain et al., "Insecure connection bootstrapping in cellular networks: The root of all evil," in *Proceedings of the 12th Conference on Security and Privacy in Wireless and Mobile Networks*, 2019.

[9] A. Singla et al., "Look before you leap: Secure connection bootstrapping for 5g networks to defend against fake base-stations," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, 2021, pp. 501–515.

[10] A. Lotto et al., "Baron: Base-station authentication through core network for mobility management in 5g networks," in *Proceedings of the 16th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, 2023, pp. 133–144.

[11] A. Bhuyan et al., "Real-world demonstration of secure 5g roaming for military communications," in *IEEE Military Communications Conference (MILCOM)*. IEEE, 2024, pp. 639–640.

[12] Trusted Computing Group, "Trusted platform module 2.0 library part 1: Architecture," Trusted Computing Group, Tech. Rep., 2023.

[13] H. Birkholz et al., "Remote attestation procedures (rats) architecture," IETF, Tech. Rep. RFC 9334, 2023.

[14] M. Ruffin et al., "Towards continuous integrity attestation and its challenges in practice: A case study of keylime," in *2025 55th Annual IEEE DSN*, 2025, pp. 256–265.

[15] L. Ferro et al., "Privacy-preserving container attestation," *Journal of Network and Systems Management*, vol. 34, no. 1, p. 5, 2026.