5G and the Need for Platform Integrity

Alec Brusilovsky[1,*] and Ira McDonald[2]

[1]*Interdigital Inc. (Manager, Security Standardization), Conshohocken, PA, USA*
[2]*High North Inc. (President), Grand Marais, MI, USA*
E-mail: alec.brusilovsky@interdigital.com; blueroofmusic@gmail.com
[*]*Corresponding Author*

Received 25 October 2019; Accepted 28 November 2019;
Publication 04 January 2020

Abstract

Current cellular architecture will not be suitable for 5G because it will not scale to the anticipated number of connected endpoints and their rich diversity. The distribution of the previously centralized Core Network (CN) functionality, e.g., Access Authentication and Authorization, has to be decentralized, leading to the demise of the most utilized tool of network security engineering, Physical Security Perimeter.

The asserted and attested Platform Integrity of the network nodes that comprise the edges of the network, the network cloud, "network fog", and the endpoints will allow mobile network operators (MNOs) to create Virtual Network Perimeters and allow highly reliable, diverse, and flexible 5G networks.

This article describes the reasons for such network transformation, provides references to applicable standardization activities, and uses the examples of support for Unmanned Aerial Vehicles (UAV) and connected automobiles by 5G networks to justify the need for Platform Integrity.

Keywords: 3GPP, 5G, AKA, BSM, DSRC, IETF, ITS, ME, MNO, OTA, RATS, RIP, SACM, SAE, SBA, TCG, UAS, UAV, UE, UTM, V2V, V2X, WAVE.

Journal of ICT, Vol. 8_1, 15–28. *River Publishers*
doi: 10.13052/jicts2245-800X.812

List of Notations and Abbreviations

3GPP	Third Generation Partnership
5G	Fifth Generation
AKA	Authentication and Key Agreement
BSM	Basic Safety Message
CN	Core Network
DSRC	Dedicated Short Range Communications
ECU	Electronic Control Unit
GP	Global Platform [7]
IETF	Internet Engineering Task Force
ITS	Intelligent Transportation Systems
ME	Mobile Equipment
MNO	Mobile Network Operator
OTA	Over-the-Air (for software updates)
RATS	IETF Remote Attestation ProcedureS WG
RIP	TCG Runtime Integrity Preservation for Mobile Devices
SACM	IETF Security Automation and Continuous Monitoring
SAE	Society of Automotive Engineers
SBA	Service Based Architecture
TCG	Trusted Computing Group [1]
TR	Technical Report
UAS	Unmanned Aerial System
UAV	Unmanned Aerial Vehicle
UE	User Equipment
UTM	UAV Traffic Management
V2V	Vehicle-to-Vehicle
V2X	Vehicle-to-Everything
WAVE	Wireless Access in Vehicular Environments [19]

1 Introduction

Several enablers will make the over-hyped promise of 5G come alive. Key features of 5G, such as the sheer number of connected endpoints and previously unheard-of diversity of these endpoints will limit the scalability of current cellular architectures. This will drive the previously centralized Core Network (CN) functionality, for instance Access Authentication and

Authorization, to become distributed and decentralized, moved to the edges of the network, the network cloud, the so called "network fog", or directly integrated in the customer endpoints.

With decentralization, the most commonly used tool of network security engineering, Physical Security Perimeter, will gradually cease to be useful.

The asserted and attested Platform Integrity of the network nodes that comprise the edges of the network, the network cloud, "network fog", and the endpoints will allow the creation of the Virtual Network Perimeter and enable highly reliable, diverse, and flexible 5G networks.

2 Trust

Trust is the belief that a person or system will behave predictably, even under stress. The following list has basic properties of trust:

- Trust is based on experience and/or evidence.
- Trust is based on fundamental properties (such as identity and integrity).
- Trust is easy to lose and hard to regain.

Based on the properties listed above, a system is considered trusted if it is predictable, even under stress, trusted based on experience and/or evidence, and trusted based on fundamental properties (e.g., identity and integrity).

3 The Need for Trusted Endpoints and Nodes

3GPP focuses on specifies protocols and standardizes to solve interoperability problems. Historically, 3GPP has "outsourced" Platform Integrity to the individual manufacturers' discretion.

The diversity and number of 5G endpoints, network elements, and services will require a new distributed security model in the network (quite different from 4G and below).

Distributed security functionality could solve the scalability problem but will still require confidence in the Platform Integrity (HW and SW) of 5G endpoints and network elements. This requirement is increased by the recent telecom industry focus on virtualization and slicing.

These security demands can be satisfied by using Platform Integrity assertions and Remote Attestations.

4 Problem Statement

Virtualization enables the migration of network functionality to the Cloud, Access Network, or Endpoint.

Virtualization introduces new security vulnerabilities due to the loss of security formerly provided by the physical protection and isolation of traditional telecom network systems.

Moving network functionality across Core Network, Endpoints, Access Network, and the Cloud, will require scalable security controls and new tools. These will provide MNO and enterprise networks with trusted ecosystems and assurance that their data and processing will remain private and uncompromised.

5G networks will require explicit and verifiable methods for protecting components (HW, guest OS, configuration, applications/library code, and data) that migrate to the Endpoints, Access Network, or Cloud.

5G networks will require standardization of trusted computing platforms (including boot, runtime, crash, and storage integrity features) to ensure interoperability. The following sections address the underlying reasons for rapidly implementing Platform Integrity techniques in 5G, describe use cases for Platform Integrity implementations, and provide references to SDOs that are now standardizing Platform Integrity.

5 Traditional 3GPP View with Reliance on Perimeter

The traditional 3GPP network security model relies heavily on the notion of a strong security perimeter with well-defined borders (e.g., firewalls) protecting critical data and infrastructure and has typically been achieved through:

- Dedicated equipment sourced by network operators from a few selected infrastructure providers.
- Placing the equipment in operator controlled physical premises with dedicated communication links.

Can this traditional model support diversity of services, business models, and endpoints for 5G?

6 Physical Network Perimeter is Gone in 5G

Network Function Virtualization (NFV) moves away from one of the main security engineering tools – physical network perimeter.

When Virtual Network Functions (VNFs) are rapidly instantiated and frequently moved from one HW/SW platform to another, trust in each HW/SW platform is of utmost importance.

There is no inherent reason not to instantiate and run a VNF on any network platform that has suitable capabilities for that VNF at a given time.

7 Platform Integrity – Why in 5G?

In the past, 3GPP never specified Platform Integrity for the Network Core, Mobile Edge, or endpoint equipment (UE). Instead, Platform Integrity was implicit and protected by the MNO's total control of physical security and ownership of the server HW/SW and the presumed security of the ME.

Such total control now conflicts with the need for Network Slicing (NS), one of the primary drivers for deployment of NFV. Practical NS is only possible when it is enabled by NFV.

TCG [1] has developed comprehensive recommendations in the new TCG Runtime Integrity Preservation in Mobile Devices [18]. These recommendations highlight hardware-assisted mechanisms that span the entire gamut from pre-boot integrity through secure boot, OS runtime monitoring, Control Flow Integrity (CFI), Data Flow Integrity (DFI), and policy-based automated fault mitigation. TCG Runtime Integrity Preservation in Mobile Devices complements traditional secure boot and measured boot technologies with its emphasis on real-time Platform Integrity, which is required for NFV and NS services.

As our mobile networks move toward 5G and tens of billions of new devices come online in the next decade, we are faced with a fundamental question of scale. Obviously, authenticating a billion devices simultaneously through a centralized function would cause even the most robust network to fail. The solution to this scalability problem is decentralization and distribution of the often privacy sensitive functionality into the "network fog", cloud, and endpoints. However, securing the mobile ecosystem – the endpoints and intermediate nodes of the telecom networks – isn't feasible in traditional ways.

8 Attestation – Know What is on the Other End

In current 3GPP specifications, the only security anchor in the UE is the UICC card (called SIM in the past and renamed SSP for the next generation).

The ME has not been authenticated traditionally. However, the USIM – a software application running on the UICC hardware platform – is only traditionally responsible for executing authentication functions and providing the symmetric session keys that are passed to the ME. Afterwards, the ME uses these session keys for integrity, confidentiality, and replay protection of its communication with the network.

While the AKA functions on the UE must be executed in the USIM that runs on the UICC platform, the network doesn't actually know where and how securely the AKA functions are executed on the UE: in the well-protected UICC; in some less protected part of the ME; on someone's laptop; or remotely in the Cloud.

To assess the overall security posture of a network node or endpoint node, assertions of the nature, security posture, location, etc. of the local and/or network authentication function are needed. Remote attestation of these assertions is required whenever the assertions are needed by a system external to the attesting platform entity.

Knowledge and confidence about what/where/how a certain Network Function is executed is a pre-condition for deployment of reliable NFV/Slicing/SBA and other complex services.

9 IETF RATS (Remote ATtestation ProcedureS) WG

"Attestation" in the IETF RATS [8] context is the process of establishing the properties of the hardware and software executing on a remote endpoint, such as the processor, device type, or OS.

The IETF RATS effort is strongly supported by participation from TCG, US NIST, Global Platform [7], FIDO, and other SDOs as well as operating system and chip vendors. TCG has already contributed documents on RATS Network Device Attestation Workflow [10] and RATS Architecture [11].

Remote endpoints can attest to the Platform Integrity of endpoints by sending trusted assertions about security-related functionality of those endpoints.

A number of ad hoc solutions already exist in this space, but SDO alignment is sorely needed on terminology, e.g., what can be considered attestation evidence, interfaces for establishing trust, and attestation data models. IETF RATS has chosen IETF JSON Web Token (JWT, RFC 7519) [16] and IETF CBOR Web Token (CWT, RFC 8392) [17] to convey the claims and evidence that comprise trusted assertions.

10 IETF SACM (Security Automation and Continuous Monitoring) WG

“Security Automation” in the IETF SACM [9] context is the process of integrating all of the security components (such as firewalls, anti-virus engines, SEIMs, Network Management Systems, etc.) into a coherent composite system that spans an entire enterprise network or telecom operator network. A SACM system continuously gathers runtime health and posture information from endpoints, intermediate systems, and servers into a central database and supports automated policy-based mitigation of issues in these network components.

The IETF SACM effort is strongly supported by participation from TCG, Global Platform, US NIST and other SDOs as well as operating system and router vendors. TCG has already contributed documents on SACM Requirements [12], SACM Software Inventory Message and Attributes (SWIMA) for PA-TNC [13], SACM Endpoint Posture Collection Profile [14], and SACM Concise Software Identification Tags [15].

11 Connected Automobiles – Need for Platform Integrity

Platform Integrity runtime monitoring, assessment, and attestation are fundamental requirements for both V2V Basic Safety Message (BSM) and V2X Over-the-Air (OTA) software update wireless communications for connected automobiles.

Current connected automobiles already contain 100 or more Electronic Control Units (ECUs). Most new automotive models are shipping with Entertainment ECUs (aka Head Units) and Telematics ECUs that support Cellular and Wi-Fi and often other wireless technologies. Automotive OEMs are deploying sophisticated technologies for assisted driving (such as collision avoidance, lane keeping, and parking assist). Automotive OEMs are designing next generation connected automobiles for autonomous applications (such as fleet vehicles and public transportation).

ITU-T, ETSI, and ISO have published Intelligent Transportation System (ITS) standards, especially for transmission of BSMs between connected automobiles and roadside infrastructure. IEEE 1609 WG has published Wireless Access in Vehicular Environments (WAVE) [19] and Dedicated Short Range Communication (DSRC) standards. SAE has published additional DSRC standards including J2735 DSRC Message Set Dictionary [20].

ITU-T, ISO, ETSI, and other SDOs have collaborated for more than a decade on development of ITS standards [21].

ITU-T has published ITU-T X.1373 [22] software update model and protocol and ISO is now developing ISO 24089 [23] software update process, both focused on OTA use cases. Automotive OEMs are currently rapidly deploying support for OTA updates for critical operational ECUs, due to steeply rising costs for automotive recalls.

12 UAV – Need for Platform Integrity

Unmanned Aerial Vehicles (UAVs) come with several extra security requirements, such as the need to bind together assertions of Platform Integrity for UEs involved in UAS, UAV Controller, and UAV Airframe along with pilot identity, pilot certificate, UAV registration, approved flight plan, and other attested values. Another key UAV requirement is the need to attest the Platform Integrity of the UEs making such assertions to the UAV Traffic Management (UTM) and also, optionally, to the 3GPP network.

Effective Platform Integrity must consider the complexity of the architecture of the use cases and the applicable networks. UAVs (or drones, as they are commonly called) illustrate this complexity. In fact, the UAV use cases are the poster children for the need of Platform Integrity and Remote Attestation.

UAVs have evolved considerably in recent years, with real-world commercial applications going far beyond their original entertainment uses. Package delivery is one application that has garnered a lot of early attention. But other use cases are being explored as well, including industrial monitoring (pipeline leak detection and inspection of roofs, wind turbines, and railway lines), public safety (flash flood warning, emergency services, and shark attack detection and prevention) and media applications in journalism and cinematography. Though all of these use cases depend on a UAV, each different application has several components that must be secured individually to complete the Unmanned Aerial System (UAS) and ensure UAV Platform Integrity.

The UAV use cases highlight the need to bind together the different assertions of Platform Integrity for the various equipment with the appropriate certifications/registrations. This requirement is more complex than it might seem on the surface. In order for the UAV to safely fly on its intended mission, all of the following elements must attest their Platform Integrity to the UAV system:

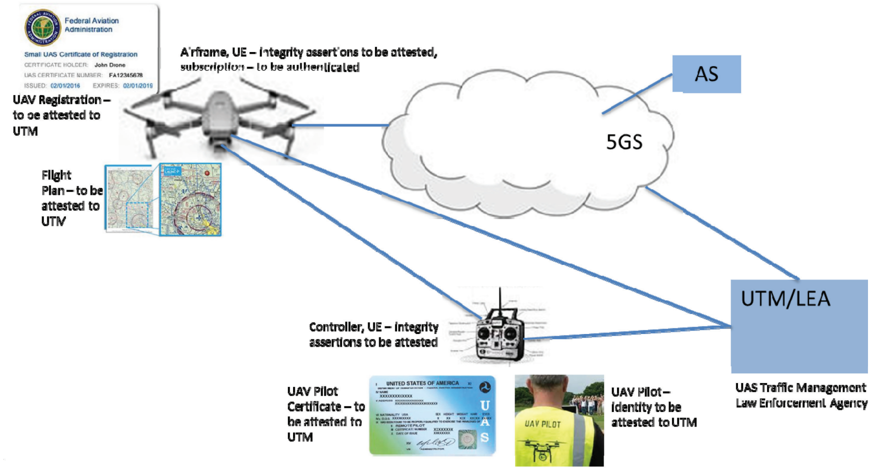

Federal Aviation Administration
Small UAS Certificate of Registration
CERTIFICATE HOLDER: John Drone
UAS CERTIFICATE NUMBER: FA12345678
ISSUED: 02/01/2016 EXPIRES: 02/01/2019
UAV Registration – to be attested to UTM
Airframe, UE – Integrity assertions to be attested, subscription – to be authenticated
Flight Plan – to be attested to UTM
5GS
AS
UTM/LEA
Controller, UE – Integrity assertions to be attested
UAV Pilot Certificate – to be attested to UTM
UNITED STATES OF AMERICA
UAS
UAV PILOT
UAV Pilot – Identity to be attested to UTM
UAS Traffic Management
Law Enforcement Agency

Figure 1 UAS architecture and key entities.

- The UAV airframe itself must have a certification and be authenticated to the UAV Traffic Management (UTM) application and also, potentially, the telecom network.
- The UAV must be registered and that registration (essentially a license plate) must be attested to the responsible UAS application.
- The approved UAV flight plan must be attested to the UTM.
- The UTM itself must implement security attestation for interworking with the MNO.
- The application servers for all applications used by the UTM system must implement security attestations.
- If the UAV is piloted, then the pilot must hold an appropriate certification/license, which in turn must be attested to the UTM to demonstrate pilot qualifications and approval.
- The UAV pilot's identity must be verified and attested to the UTM.
- The UAV controller module ("remote control") device must implement security attestation.
- UAV payloads (e.g., dangerous or hazardous cargo cases) must have security attestations as well.

For the UAV to fly in a truly secure system with complete Platform Integrity, all of these aspects of the system must match expected values – for example, the UAV pilot's license be in good order – and be cryptographically bound together. If one aspect does not match expected values, then the UAV should not be allowed to take off. Further, the UTM or an appropriate law enforcement agency must be able to override the UAV controller in the event of a breach of Platform Integrity or a violation of the pre-filed flight plan, because in the air anything can happen: a device could malfunction, a pilot could become distracted, or a strong wind could blow an airborne UAV into the airspace of an airport or other secure facility. In any of these exception cases, it’s important to ensure the UAV can make a safe landing without risking anyone’s safety.

Various communications and command and control systems must be considered, because each contributes to the overall UAS Platform Integrity. Air traffic control communications, UAV telemetry systems, and vehicle-to-vehicle communications systems each must have appropriate security and Platform Integrity attestation in a functioning UAS.

UAVs are only the first of many systems that will require such an approach to Platform Integrity. As we move further along our 5G journey, we’ll see similar distributed security models in connected cars, telemedicine and medical devices, and a range of mission-critical and vertical industrial applications. Although some of these scenarios may seem futuristic today, use cases like the UAV/UTM example above are already being examined by major standards organizations, so these Platform Integrity considerations are likely to be included in future cellular technology standards.

3GPP already plans to standardize 3GPP enhancements for UAV/UAS support in [2–4], Service Requirements. While [5] contains proposals for architectural improvements for the application layer and [6] (currently, just a shell of a TR) will address 3GPP architectural and procedural improvements for support of UAV/UAS.

12.1 UAS Terminology

Unmanned Aerial Vehicles (UAV) – Commonly known as Drones, Remotely piloted aerial vehicles (RPAVs), Remotely piloted aircraft (RPA), etc.

Unmanned Aerial System (UAS) – UAS emphasizes the importance of other elements beyond UAV itself. UAS includes ground control stations, communication infrastructure, management entities and other related support infrastructure.

National Air Space (NAS) – NAS includes the airspace, navigation facilities and airports along with services, rules, regulations, policies and procedures.

UTM (UAV Traffic Management) – A civilian Low-Altitude Airspace for UAS Operations analogous to the system of roads, lanes, stop signs, lights, and rules that governs automobile traffic today.

13 Conclusion

As time progresses, technology changes, and standards evolve, so too will our methods of ensuring system and network security evolve. For these complex systems comprised of so many human and technological components using different protocols, communication media, computing platforms, and software defined ultra-low latency 5G networks, it's clear that our traditional model of Physical Perimeter Security is simply insufficient. Modern Platform Integrity technologies will enable us to realize the opportunities of the 5G by deploying Virtual Perimeter Security that supports both security and safety requirements specified in standards and regulations.

In the future, strong endpoint Platform Integrity will be the foundation of security in the UE (e.g., both ME and UICC/SSP components), automotive head units and telematics, UAV security/communication modules, Mobile Edge Computing (MEC) systems, and telecom infrastructure servers. Assurance of Platform Integrity will be required for most 5G/IoT/Cloud deployments. Therefore, TCG, GP, and IETF RATS are quickly developing technologies capable of delivering Platform Integrity assurance.

Acknowlegdements

Authors would like to acknowledge Ravikumar (Ravi) Pragada and Arnab Roy for sharing their UAV industry expertise and Samir Ferdi for 5G Core Network insights.

References

[1] Trusted Computing Group (TCG) http://www.trustedcomputinggroup.org/
[2] TS 22.125 Unmanned Aerial System (UAS) support in 3GPP.
[3] TR 22.829 Enhancement for Unmanned Aerial Vehicles (UAVs).
[4] TR 22.825 Study on Remote Identification of Unmanned Aerial Systems (UAS).

[5] TR 23.754 Study on supporting unmanned aerial systems connectivity, Identification and tracking.

[6] TR 23.755 Study on application layer support for Unmanned Aerial Systems (UAS).

[7] Global Platform (GP) http://www.globalplatform.org/

[8] IETF Remote Attestation Procedures WG https://datatracker.ietf.org/wg/rats/about/

[9] IETF Security Automation and Continuous Monitoring WG https://datatracker.ietf.org/wg/sacm/about/

[10] RATS Network Device Attestation Workflow https://datatracker.ietf.org/doc/draft-fedorkow-rats-network-device-attestation/

[11] RATS Architecture https://datatracker.ietf.org/doc/draft-birkholz-rats-architecture/

[12] SACM Requirements https://tools.ietf.org/html/rfc8248

[13] SACM Software Inventory Message and Attributes (SWIMA) for PA-TNC https://tools.ietf.org/html/rfc8412

[14] SACM Endpoint Posture Collection Profile https://datatracker.ietf.org/doc/draft-ietf-sacm-ecp/

[15] SACM Concise Software Identification Tags https://datatracker.ietf.org/doc/draft-ietf-sacm-coswid/

[16] IETF JSON Web Token (JWT) https://tools.ietf.org/html/rfc7519

[17] IETF CBOR Web Token (CWT) https://tools.ietf.org/html/rfc8392

[18] TCG Runtime Integrity Preservation in Mobile Devices https://trustedcomputinggroup.org/wp-content/uploads/TCG_MPWG_RIP_r105_pubrev.pdf

[19] IEEE Wireless Access in Vehicular Environments (WAVE) https://standards.ieee.org/standard/1609_0-2019.html

[20] SAE J2735 Dedicated Short Range Communication (DSRC) Message Set Dictionary https://www.sae.org/standards/content/j2735_200911/

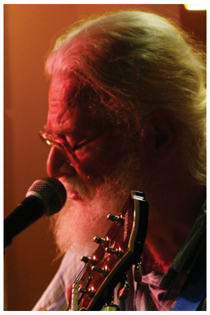
[21] ITU-T Collaboration on ITS Communication Standards https://www.itu.int/en/ITU-T/extcoop/cits/Pages/default.aspx

[22] ITU-T X.1373 Secure software update capability for intelligent transportation system communication devices https://www.itu.int/rec/T-REC-X.1373/en

[23] ISO 24089 Road vehicles—Software update engineering, work-in-progress https://www.iso.org/standard/77796.html

Biographies

Alec Brusilovsky is Manager, Security Standardization at Interdigital. He has extensive experience in security architecture, design, consulting, and applications development for wireline, wireless and IP networks for the key operator, as well as the major vendor. His interests include NFV security, platform integrity, security and privacy for 5G Wireless Networks and associated standardization issues.



Ira McDonald is President of High North Inc. He has been a consulting cybersecurity architect at automotive OEMs, network equipment vendors, telecom operators, and printer manufacturers since 1973. He is co-founder of the IEEE-ISTO Uptane Alliance project for secure automotive firmware updates. He wrote Mitsubishi FOTA cybersecurity standards and also wrote FCA Internet Security, Ethernet Security, TLS Security, FOTA, and IDS cybersecurity standards. He has been an officer and editor in IEEE, IETF, ISO, DMTF, SAE, TCG, and Linux Foundation standards projects since 1994.