Technical Disclosure Commons

Defensive Publications Series

May 2022

NOVEL METHOD FOR CAPTURING, STORING, AND EXCHANGING SECURITY KEY PERFORMANCE INDICATOR (KPI) DATA FOR 5G NETWORK SLICING

Prapanch Ramamoorthy

Akshay Dubey

Vijay Venugopal

Selina Sun

Recommended Citation

Ramamoorthy, Prapanch; Dubey, Akshay; Venugopal, Vijay; and Sun, Selina, "NOVEL METHOD FOR CAPTURING, STORING, AND EXCHANGING SECURITY KEY PERFORMANCE INDICATOR (KPI) DATA FOR 5G NETWORK SLICING", Technical Disclosure Commons, (May 09, 2022)
https://www.tdcommons.org/dpubs_series/5125

NOVEL METHOD FOR CAPTURING, STORING, AND EXCHANGING SECURITY KEY PERFORMANCE INDICATOR (KPI) DATA FOR 5G NETWORK SLICING

AUTHORS:
Prapanch Ramamoorthy
Akshay Dubey
Vijay Venugopal
Selina Sun

ABSTRACT

Network slicing is a key capability provided to Fifth Generation (5G) mobile network operators. The industry has defined many predefined network slice types that depend on various key performance indicators (KPIs) such as bandwidth, throughput, and latency. However, one missing component, in terms of KPIs for defining network slices, is security, as there is currently no mechanism to translate network security or segmentation of traffic into a 5G core network or Radio Access Network (RAN). Presented herein are techniques to enable micro segmentation of a 5G network by using security as a KPI. The techniques provided herein can be achieved by leveraging existing security capabilities and algorithms to determine a reputation of endpoints and embedding the reputation within a slice differentiator.

DETAILED DESCRIPTION

Network slicing is a key concept in the Third Generation Partnership Project (3GPP) Fifth Generation (5G) System (5GS) architecture. A network slice is a logical end-to-end network that can be dynamically created and may include any combination of 3GPP mobile core network functions/functionality.

A user equipment may have access to multiple network slices over a Radio Access Network (RAN). Each network slice may serve a particular service type with an agreed upon Service-level Agreement (SLA). To provide mobile network services associated with a given slice type, a slice of the given network slice type can be instantiated in which the instantiated slice for the slice type can provide certain mobile network services to a number of UEs.

Per-3GPP Technical Specification (TS) 23.501, Section 5.15.2, Single-Network Slice Selection Assistance Information (S-NSSAI) can be used to uniquely identify a slice in which an S-NSSAI includes a Slice/Service Type (SST) indication, which indicates the expected slice behavior for a slice requested by a UE in terms of expected features and services, and, optionally, can include a Slice Differentiator (SD), which can be used to differentiate among multiple slices of a same SST.

Different types of slices (slice types) can be configured for a mobile network such that each slice type can provide certain mobile network services. Various example slice types can include, but not be limited to, a cellular vehicle to everything (V2X) slice type that can provide cellular V2X services, an Internet of Things (IoT or IOT) massive IoT (mIoT) slice type that can provide IoT related services, an Ultra-Reliable Low-Latency Communication (URLLC) slice type that can provide URLLC services, an enhanced Mobile Broadband (eMBB) slice type that can provide mobile broadband services, a massive Machine-Type Communication (mMTC) slice type that can provide MTC services, a High Performance Machine-Type Communication (HMTC) slice type that can provide HMTC services, etc.

Many predefined network slice types exist that depend on various key performance indicators (KPIs) such as bandwidth, throughput, and latency. However, one missing piece of current network slice definitions is security. Traditional network deployments (wireless or wired) have shown the importance of baking in security into a network design. For example, in terms of network segmentation, many solutions exist in traditional networks such as virtual local area networks (VLANs), security or scalable group tags, etc. While all of these technologies can continue to exist in the core parts of a network, there is currently no such mechanism to translate this into part of the 5G network such as the RAN and Core.

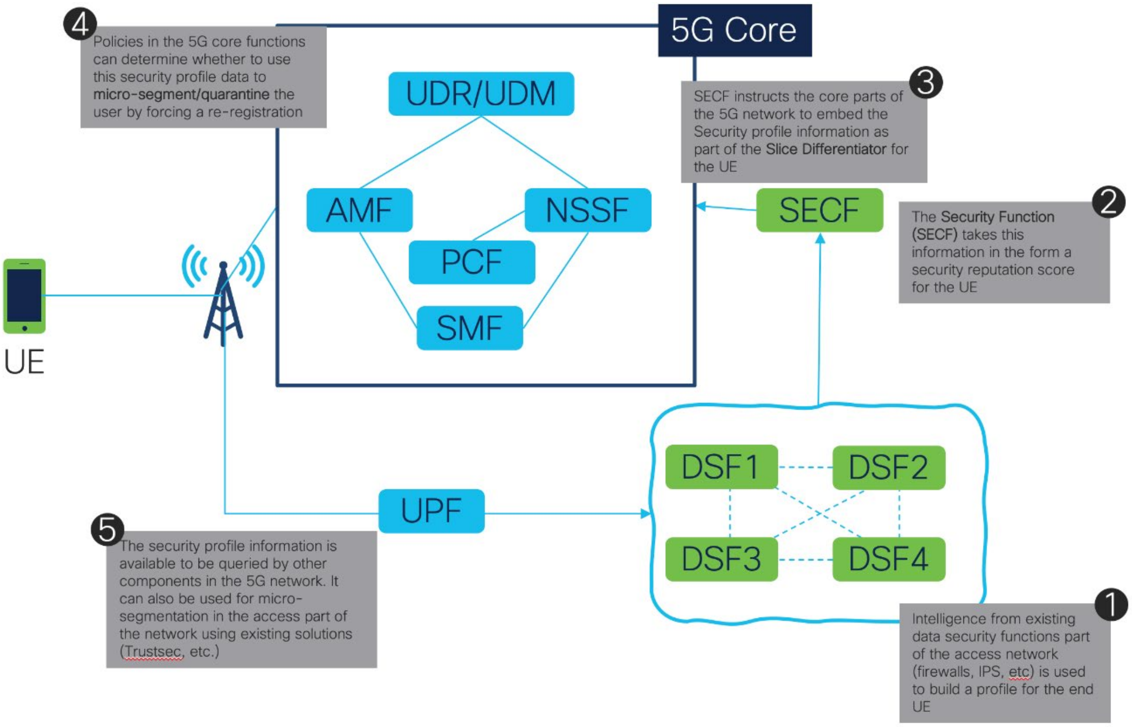
Proposed herein is a novel technique for carrying security-related information leveraging the network slicing framework available in 5G mobile networks.

Per 5G 3GPP standards, the role of determining the network slice for a particular 5G UE is that of a Network Slice Selection Function (NSSF) in which each unique network slice is identified by an S-NSSAI field. As defined in the standards, this is a 32-bit field allocated as:

- 8-bits for SST; and

- 24-bits for the optional SD, which can be used by 5G mobile network operators (MNOs) to differentiate between slices of the same type.

The SD plays a key role in the techniques proposed herein, as shown below in Figure 1, which illustrates an example architecture through which techniques of this proposal may be implemented. Although a single UE is illustrated in Figure 1, it is to be understood that any number of UEs can be connected to a 5G network.



4 Policies in the 5G core functions can determine whether to use this security profile data to **micro-segment/quarantine** the user by forcing a re-registration

3 SECF instructs the core parts of the 5G network to embed the Security profile information as part of the **Slice Differentiator** for the UE

2 The **Security Function (SECF)** takes this information in the form a security reputation score for the UE

5 The security profile information is available to be queried by other components in the 5G network. It can also be used for micro-segmentation in the access part of the network using existing solutions (Trustsec, etc.)

1 Intelligence from existing data security functions part of the access network (firewalls, IPS, etc) is used to build a profile for the end UE

Figure 1: Example 5G Network Architecture

With reference to Figure 1, depending on the Policies defined and the NSSF, each of a given UE can be placed into its own unique network slice type using a unique value of SST (e.g., 1 for eMBB, 2 for URLLC, 3 for mMTC, 4 for enterprise 1 slice, etc.). During operation, each of these unique slice types will have a large number of UEs connected to them.

For example, consider for Figure 1 that two UEs, UE1 and UE2, are connected to an enterprise slice and they both are mobile handsets of users. At this stage, the registration process has been completed and the two UEs have the ability to connect to the access network. In the access network, there is likely to be a combination of various data security functions/services (DSFn, in Figure 1), which could encompass be firewalls, intrusion prevention systems, anomaly detection functions, malware protection services, email filtering, etc.

Data from the UEs would be inspected by a multitude of DSFs, using algorithms as currently known in the art, and insights provided by the DSFs could culminate in a decision regarding a security reputation/score of a particular endpoint. It is to be understood that techniques described herein are not limited to any particular method/algorithm for computing/determining a security score/reputation, but rather can leverage any static, user defined/configured, and/or dynamic method of determining a security reputation.

Initially the UEs will have an unknown reputation score and could then be assigned a different reputation score based on the analysis of their network traffic pattern. For example, after a certain time, UE1 could be given a high score (implying there is no evidence of malicious network traffic patterns) and UE2 could be given a low score (implying that there has been evidence of certain malicious traffic, e.g., UE2 has downloaded a known malware file or has accessed websites that carry a poor reputation score).

In accordance with techniques herein, this information can be communicated to a Security Function (SECF), which is part of the 5G core. In some instances, this role could be played by an existing centralized security management solution or an integrated solution. A key function of the SECF is to be able to consume a change in the security reputation of one or more UEs and translate change to a security score that can be embedded in the SD part of the S-NSSAI.

For example, as illustrated in Figure 2, below, an "isolation" field can be configured within the SD field of the S-NSSAI and can be used to indicate whether to place a particular UE in a quarantined network slice. Further, a "security profile" field can be used to provide a representation of the reputation of the particular UE, computed and communicated based on the insights provided by the DSFs. Additionally, a "reason" filed can be used to carry a reason why the particular UE has been given a particular security score.

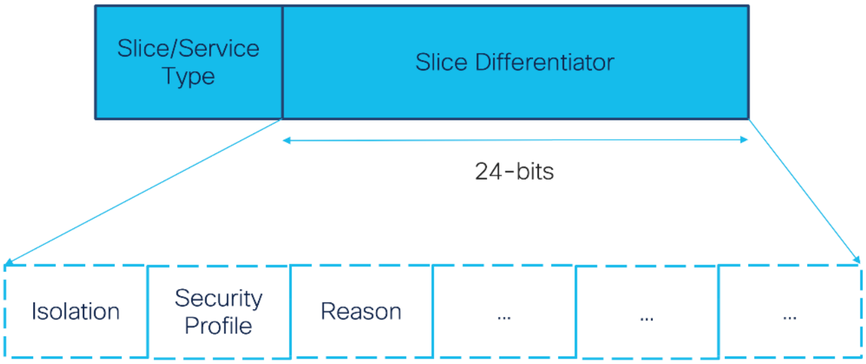


Figure 2: Slice Differentiator Configured to Carry Security Information

In accordance with the techniques proposed herein, the SECF can be configured by a network administrator/operator with policies to map different security reputations to specific values for the corresponding fields of an SD, as illustrated above in Figure 2.

During operation, the SECF can obtain this information for the SD and communicates it to the NSSF so that a given UE can now be differentiated into its own unique network slice within the SST in which it was placed into originally. In some instances, there could be policies defined in a Policy Control Function (PCF) that trigger application of policies for a given UE based on the information in the SD. For example, if the "isolation" field is set for a particular UE, the UE could be forced to re-register and be placed to a quarantine part of the 5G network including the RAN, Core, etc. so as to not affect other UEs in the same network. Similarly, the other fields could be used for further micro-segmentation of the 5G network based on the embedded security information in the SD.

Further, the availability of a security KPI as part of the SD can be used by other parts and functions in a 5G network in order to make decisions as to the Quality of Service (QoS) provided to users in order to enforce bandwidth, throughput, security policies, etc. Still further, the information in the SD can be translated to other forms of micro-segmentation within the access network, such as through the use of trusted security group tags and/or the like.

Reputation scores can be determined/updated continuously over time. For example, as traffic is obtained from users, the DSFs will continue to inspect and analyze the traffic in order to provide additional insights. The insights from the DSFs can continue to be used to compute the overall reputation of UEs based on existing algorithms and communicated to the SECF. The policies in the SECF will be continuously evaluated and actions taken if there is a change in the reputation and the policy mandates the need to modify the SD for a particular UE. As an SD is changed due to changes in the security profile of a given UE, changes in the S-NSSAI configuration may also be needed at multiple places in the 5G core network (e.g., PCF, NSSF, etc.) in order to ensure consistent application of policies across different users. As an alternative to updating SDs as reputation scores change over time, in some instances a single SD could be defined into which users could be quarantined if their reputation score fell below a threshold, which could help to alleviate potential configuration changes for S-NSSAIs throughout a network.

Accordingly, techniques presented herein provide a novel method for embedding security as a KPI within a 5G network using the SD field of the SNSSAI. This information can be used by various functions to enforce policies when it comes to throughput, security policies to enforce, isolation, etc. By providing such features, techniques herein may enable further micro-segmentation of users for different elements of 5G networks. Moreover, the embedded security information as part of the SD can be used by various 5G functions for various policy applications that provide an overall quality of service for end users.