Security Requirements for Multi-operator Virtualized Network and Service Orchestration for 5G

10

Mateus Augusto Silva Santos, Alireza Ranjbar, Gergely Biczók, Barbara Martini, and Francesco Paolucci

10.1 Introduction

The next generation of communications systems, 5G, will enable the deployment of diverse services with different networking requirements. Unlike earlier generations which consider a general purpose network for all services, 5G will be able to assign network services based on specific networking needs. As it is envisioned by the 5G-PPP community, 5G will empower a diverse set of verticals such as factories of the future (FoF), health, automotive, and media and entertainment. In order to enable the deployment of differentiated capabilities, 5G employs the end-to-end network slicing approach based on virtualized resources [2, 3]. These slices require multi-operator orchestration at both the business and technical levels. From the business point of view, operators should negotiate and agree on a set of services that they are

M.A.S. Santos (✉)
Ericsson Telecomunicações S/A, Rod. Eng. Ermênio de Oliveira Penteado, Km 57.5, 13337-300, Indaiatuba, Brazil
e-mail: mateus.santos@ericsson.com

A. Ranjbar
OY L M Ericsson AB, Hirsalantie 11, Jorvas, Finland
e-mail: alireza.ranjbar@ericsson.com

G. Biczók
CrySyS Lab, Department of Networked Systems and Services, Budapest University of Technology and Economics, Budapest, Hungary
e-mail: biczok@crysys.hu

B. Martini
Consorzio Nazionale Interuniversitario per le Telecomunicazioni (CNIT), Pisa, Italy
e-mail: barbara.martini@cnit.it

F. Paolucci
Scuola Superiore Sant'Anna, Pisa, Italy
e-mail: fr.paolucci@sssup.it

S.Y. Zhu et al. (eds.), *Guide to Security in SDN and NFV*, Computer Communications and Networks, DOI 10.1007/978-3-319-64653-4_10

able to provide. From the technical point of view, operators should be able to assign (virtual) resources to services in an agile and flexible manner. Technologies such as NFV and SDN are key enablers for providing high flexibility and manageability in service allocation and orchestration through 5G slices. Moreover, since end-to-end 5G slices may span across different operators, security becomes of utmost importance. Operators should be able to negotiate and deliver services without revealing sensitive configurations or part of their virtual or physical resources to others. In addition, end-to-end slices may require high level of isolation at the control, management, and also at the resource layer. Some control operations of each slice may need to be isolated from other slices, and there should be a way to authenticate and monitor a large number of virtual services deployed across multiple operators.

In the following, we review SDN and NFV as key technologies in 5G and introduce our 5G multi-operator service orchestration architecture.

10.1.1 The Role of NFV and SDN in 5G

NFV and SDN will be an important part of 5G enabling the flexible, rapid, and cost-efficient deployment of network services. NFV decouples software from hardware and provides higher resource efficiency and scalable service deployability by virtualizing the network functions and resources. The virtualized services can be deployed on demand to achieve higher coverage or capacity. Another major benefit of NFV is that it allows operators to implement network services independent of the location. In fact, virtualized services are not anymore bounded to physical networks, and depending on the desired functionality, they can be implemented close to base stations (i.e., at the edge) or on a centralized data center.

While NFV is focused on virtualizing the network functions, SDN aims at offering a higher level of control over network resources by centralizing the control and management functions. SDN separates the control plane from the data (forwarding) plane; the control plane consists of a logically centralized and programmable controller, which has an abstract view of network resources. The higher programmability and abstraction in SDN allow operators to define customized 5G logical slices with different sets of services. NFV and SDN are complementary technologies in 5G. In fact, SDN can be part of NFV framework, particularly to enhance the controllability and manageability of NFV components.

10.1.2 Multi-operator Orchestration Architecture

In order to have a common view of 5G resource sharing and orchestration between operators, the 5GEx innovation project [1] proposed a hierarchical architecture shown in Fig. 10.1. At the highest level, customers and operators negotiate and agree on services; at the lowest level, virtual and physical network resources are assigned to customers.

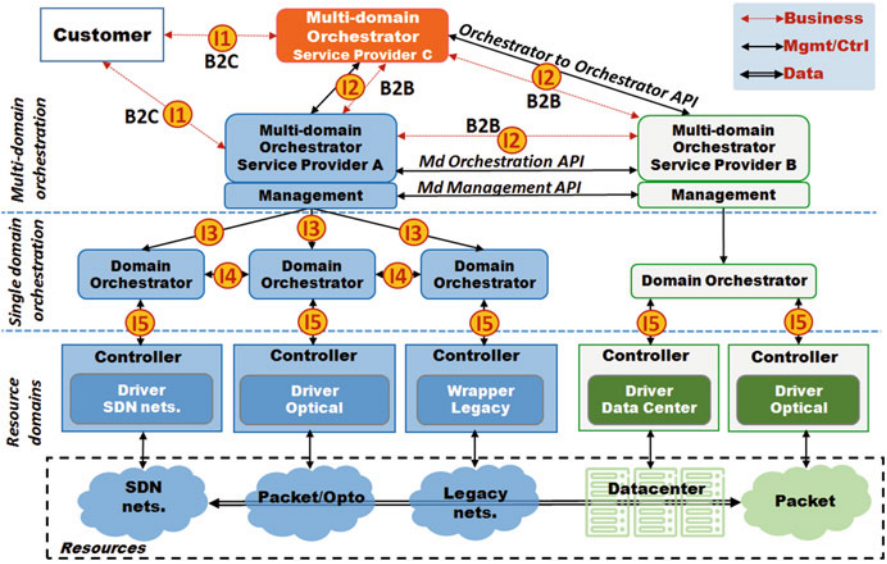

Fig. 10.1 5GEx multi-operator orchestration architecture [16]

The architecture illustrates the relation between different entities with a set of interfaces (I1 to I5). In this architecture, business agreements between an operator and a customer (i.e., business-to-customer, B2C) will happen through interface I1, while the operators negotiate (i.e., business-to-business, B2B) for service allocation through interface I2. Based on the agreements, the management entity in each provider network will request the domain orchestrators through interface I3 to map resources to a specific network slice. To offer end-to-end services, domain orchestrators may interact with each other through interface I4. Lastly, domain orchestrators instruct controllers to assign resources based on the technology deployed in the domain (e.g., SDN, optical, etc.). It is important to emphasize that the 5GEx project focuses on interfaces I1, I2, and I3.

The interaction between multi-domain orchestrators (MdOs) enables a service to be orchestrated in a multi-provider environment. Specifically, MdOs enable VNF instantiation on a third-party infrastructure through two fundamental components: Network Service Orchestrator (NSO) and Resource Orchestrator (RO) [11]. NSO manages the life cycle of network services in coordination with VNF Managers. RO provides an overall view of the resources within an administrative domain. An interesting observation is that operators' ROs can interact to expose slices in an abstracted and unified view which can be consumed by an NSO that will expose services to a customer. Thus, the split architecture of an MdO allows use cases such as network services provided using multiple administrative domains (i.e., multiple NSOs that compose services using cross-domain VNFs) as well as a network service provided using multiple infrastructure providers (i.e., multiple ROs expose a virtual

data center to an NSO). We refer to the use cases #1 and #3 as defined in [11] for more specific examples and descriptions.

In the next section, we discuss in more details the security requirements of the 5G multi-operator architecture, and, particularly, we will focus on the security of NFV and SDN as key enabling technologies for 5G. We consider the functional split of MdOs to provide a more detailed analysis.

10.2 Security Perspectives from Standards Organizations

To elaborate the security requirements of multi-operator service orchestration, we first review the security architecture provided by ITU-T X.805 standard, and then, we apply ITU-T security recommendations to interfaces of the 5GEx multi-operator architecture shown in Fig. 10.1. In addition, we also review some of the ETSI NFV recommendations for security of multi-operator service orchestration in the following of this section.

10.2.1 ITU-T X.805

The ITU-T X.805 [17] provides recommendations for end-to-end network security regardless of the underlying networking technology. Even though it was published more than a decade ago, the recommendations are still very useful to understand potential types of protection needed against threats. The reason stems from the fact that the X.805 architecture is generic enough to accommodate the existing challenges in network security, as we explain next.

X.805 Security Architecture. Figure 10.2 shows the X.805 security architecture, which comprises three architectural components: security dimensions, security layers, and security planes. Eight security dimensions are used to measure specific aspects of network security. Three security layers (infrastructure, applications, and services) provide a hierarchical structure for applying the security dimensions to certain categories of network resources. Three security planes (management, control, end user) consist of a particular group of network activities that should be protected by security dimensions.

The infrastructure security layer measures the security in network components (i.e., switches and routers) and their communication links. The services security layer applies security at services offered by a service provider, while the applications security layer addresses the security of network-based applications. Since security for multi-operator networks is dealing with services, we only need to apply the security dimensions to the services security layer in the scope of each security plane.

According to the X.805 standard, the concept of protecting a network by security dimensions at each security plane provides a comprehensive security solution. As illustrated in Fig. 10.3, different security dimensions protect security planes. Focusing on the services security layer, we can define the security planes as follows [17]:

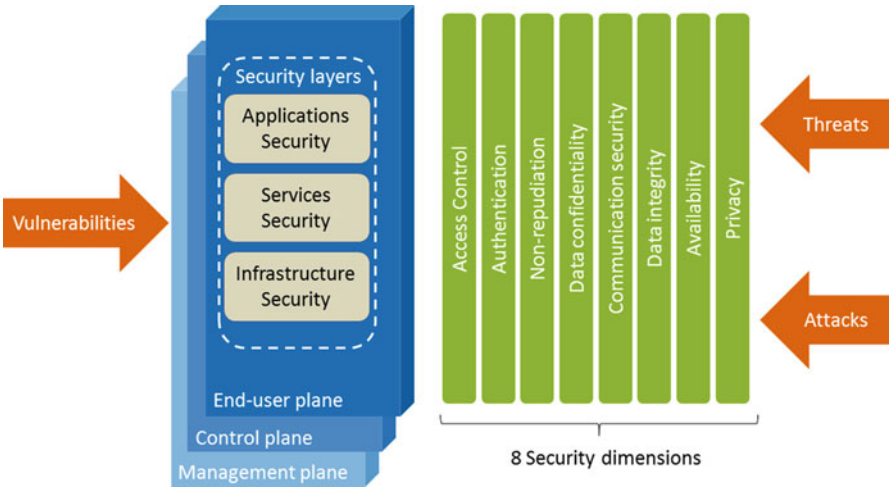

Fig. 10.2 X.805 security architecture

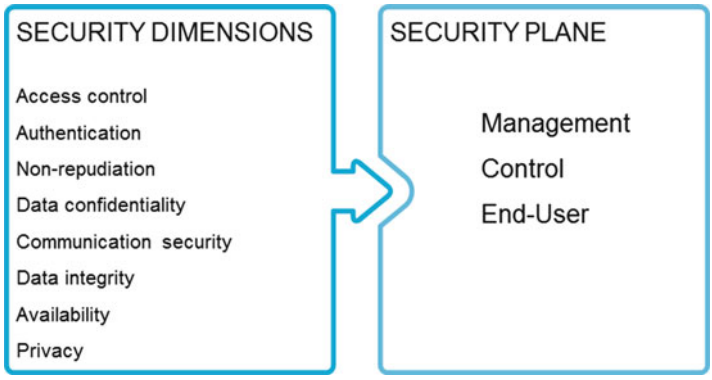

Fig. 10.3 Architecture rationale: security dimensions protect security planes

- Management plane: concerned with securing the operations, administration, maintenance and provisioning functions of network services.
- Control plane: securing the control or signaling information used by a network service, including control messages of network devices participating in the service.
- (End-)user plane: securing user data as it uses a network service. In the context of multi-operator networks, the term "user" is the same as "customer" in Fig. 10.1, which refers to either a service provider or an enterprise customer. We replace the term end-user plane by user plane.

We now review and discuss security for each dimension by observing the aforementioned planes. We group the security dimensions previously mentioned with conceptual intersections such as authentication and integrity with non-repudiation, and data confidentiality with privacy.

Authentication, Integrity, and Non-repudiation. X.805 states that data integrity protects the information of network services against unauthorized modification, deletion, creation, and replication. Non-repudiation is enabled by providing a record, which identifies activities performed. We highlight that information is defined according to the security planes mentioned earlier. Authentication ensures that claimed identities are verified.

Data integrity and non-repudiation can be provided by using a hash chain; essentially the successive application of a cryptographic hash function. Since such method provides onetime signatures, it is well suited for protecting management information, e.g., keeping track of management activities or past logs. Connection-oriented interactions between MdOs, including control information exchange, could be better secured with public-key cryptography schemes such as digital signatures. Such a method provides authentication, integrity, and non-repudiation.

Table 10.1 shows the security planes as well as the 5GEx-related interfaces that can be protected in the context of authentication, data integrity, and non-repudiation. Note that we only consider the security of interfaces I1, I2, and I3, since they are the focus of the 5GEx project.

Access Control. Access control ensures that only authorized identities or devices are allowed to access services. This security service can be provided with authentication servers, following an adapted version of the IEEE 802.1x framework. Access control can also be provided by using encryption and role-based controls. A policy

Table 10.1 Authentication, integrity, and non-repudiation combined with the security planes of X.805

Planes	Data authentication, integrity, and non-repudiation	Interfaces affected and possible countermeasures
Management	Protect management information and provide a record identifying management activities performed	I1, I2 for service management and VNF life cycle management. Protection with digital signatures or hash chains
Control	Protect control information and provide a record identifying the origin of control messages. Verify identity that originates control information	I1, I2 for service exposure. I2, I3 for resource orchestration. Protection with digital signatures
User	Protect user data being transported, verify its origin, and provide a record identifying each user and device that accessed and used the network service and the action that was performed	Not directly applicable

Table 10.2 Access control combined with the security planes of X.805

Planes	Access control	Interfaces affected and possible countermeasures
Management	Ensure only authorized identities are allowed to perform management activities of the network service	I1, I2 for requesting the instantiation and configuration of VNFs and SLA management. Protection can be provided with encrypted requests or authentication servers
Control	Ensure that control information for a network service originates from an authorized source before accepting it	Not directly applicable if user service request is granted and persisted
User	Ensure that only authorized users and devices are allowed to access and use the network service	I1 for requesting services. Protection with authentication servers that persist the authorization

Table 10.3 Data confidentiality and privacy combined with the security planes of X.805

Planes	Data confidentiality and privacy	Interfaces affected and possible countermeasures
Management	Protect the network service's configuration and management information. Ensure that no information can be used to identify the network management service system	I1, I2 for service management and VNF life cycle management. Protection with encryption
Control	Protect network service control information. Privacy for network devices or communications links participating in a network service	I1, I2 for service exposure I2, I3 for resource orchestration. Protection with encryption
User	Protect user data that is being transported, processed or stored by a network service against unauthorized access or viewing. Privacy for information pertaining to the user's use of the service	Not directly applicable per interface. Still an existing trust issue (with regard to user data flowing through a provider without having an established relationship)

database could be provided for user access differentiation. Table 10.2 shows how the security planes can be applied to 5GEx in the context of access control and authentication. We emphasize that only interfaces I1, I2, and I3 are taken into account.

Data Confidentiality and Privacy. Confidentiality protects the information from unauthorized access or viewing. Privacy ensures that no information will be available to be used to identify the network service. Encryption schemes are useful for implementing confidentiality and privacy. Table 10.3 shows the 5GEx interfaces that could be affected by the security planes for data confidentiality and privacy.

Availability. The availability security dimension ensures that there is no denial of authorized access to services. Considering that access policies are effective,

Table 10.4 Availability combined with the security planes of X.805

Planes	Availability	Interfaces affected and possible countermeasures
Management	Ensure the ability to manage network service cannot be denied for authorized entity	I1, I2 for SLA management, VNF instantiation and configuration as well as VNF life cycle management. Protection with multiple NSOs
Control	Ensure that network devices participating in a network service are always available to receive control information from authorized sources	I2, I3 for resource orchestration. Protection with multiple ROs
User	Ensure no denial of access to the network service by authorized users	I1 for request of services. Protection with multiple NSOs

availability can be provided by using logically centralized and physically distributed orchestrators per administrative domain. Table 10.4 presents the 5GEx interfaces affected in the context of availability.

10.2.2 ETSI NFV

ETSI Network Functions Virtualization (NFV) Industry Specification Group (ISG) provides technical recommendations and standards for the adoption of NFV, based on the network operator requirements. The ETSI NFV ISG has published a list of security issues [9] which we discuss next with respect to the multi-operator networks while taking into account ETSI's recommendations on security [8]. It should be noted that other concerns about security of individual network elements or VNFs are out of the scope of this document.

Topology Validation. Operators should be able to validate the connectivity between all network elements; however, this process is often complex especially because of the large number of virtualized functions. The topology validation of VNFs is particularly important considering the end-to-end slices in 5G, which require VNF orchestration across several virtual networks. Operators should verify that the network connectivity satisfies the forwarding policy of VNF chains and each VNF deploys the intended functionality. Also, it should be verifiable that the VNFs are connected to the correct virtual network and the topology of VNFs should be free of loops, which could be introduced accidentally or maliciously.

To improve VNF chaining across different operators, multi-domain orchestrators should be able to instruct local SDN controllers to set up a path for a specific chain of VNFs. However, orchestrators are expected to possess an abstract view of network topology. Depending on the level of abstraction, the ability of computing specific paths for VNFs is limited, leaving such task to an SDN controller. Moreover, the SDN controller becomes a trusted entity to hold information about physical and

virtual network resources. As a consequence, if not secured, attackers may break into the centralized controller and gain access to the physical and virtual topology information.

Performance and Network Isolation. Considering the 5G multi-operator scenario in which a service spans across multiple administrative domains, virtual networks might be deployed on several shared physical resources. Therefore, it is important to isolate the virtual networks by creating logical slices across all operators involved in the service. End-to-end slices will require a standardized interface between multi-domain orchestrators so that each operator may provide its own performance characteristic and network isolation method.

Multi-Administrator Isolation. The hierarchy of administrators can become a potential source of threats when it comes to delegation of control or privileges between orchestrators of different administrative domains. It is important to consider the privileges of administrators of virtualized networks and functions.

User/Tenant Authentication, Authorization, and Accounting (AAA). The multilayer virtualization introduced by NFV may lead to AAA-related issues. Authentication may lead to the disclosure of end-user's identities in a federation of different NFV infrastructure providers. One solution is to validate all identity tokens in VNF layers. Authorization can also introduce new privilege challenges, as it requires rich policies to identify the authorized users and tenants. The deployment of accounting for resource usage and billing purposes can also be challenging especially because the VNFs may be deployed at/by different operators. This requires granular traffic classification and accounting between orchestrators.

Back-Doors via Virtualized Test and Monitoring Functions. Operators may provide a set of monitoring interfaces which can be used remotely for provisioning, configuring, debugging, and testing the VNFs. While operators may give certain privileges to each other, for example, for performance and quality monitoring, these interfaces should be properly hardened and restricted against any unauthorized access by attackers or even by other operators.

10.3 Threat Analysis Method

We provide a threat analysis over multi-operator networks according to the method illustrated in Fig. 10.4. Using a multi-provider scenario to specify interactions, we consider a selective list of threats and their reasons. Then, we provide a list of potential security schemes that can protect the system against the threats. Standards are also considered based on the study in Sect. 10.2. Finally, we elaborate on gaps identified from schemes and standards.

Fig. 10.4 Proposed method for threat analysis

10.3.1 Multi-provider Scenario

In order to understand the security aspects of a multi-provider environment, we consider the scenario of a wholesale infrastructure service, combining network, storage, and compute resources from multiple operators. A given service provider, SP_A, can create a service that involves other service providers' infrastructure in a process that consists of the following steps:

1. Customer sends a service request to SP_A;
2. SP_A MdO decomposes the service into smaller service components;
3. SP_A MdO maps service components to an inter-provider resource topology, defining the SPs that will cooperate to deliver the network service and their respective resources;
4. SP_A MdO sends requests to other SPs MdOs involved in order to instantiate the service components required (e.g., compute, storage).

Figure 10.5 illustrates the scenario. 5GEx Interface 1 (I1) is used in the first step of the aforementioned process, while the other steps are mostly defined in Interface I2 (I2). Examples of control messages that should be exchanged between MdOs are advertisement of resource topology and service catalog. The former exposes available resources that a service provider intends to share and the latter exposes available services. Exchange of control data between peers of MdOs is subject to threats that we elaborate in the next sections.

10.3.2 Threat List and Reasons

Before discussing threats and their reasons, it is important to understand the relationship between an orchestrator and an SDN controller in terms of security. Threats to an SDN controller can affect its corresponding orchestrator, and vice versa.

An orchestrator usually operates right atop an SDN controller using a defined interface for communication in the hierarchy. Such method is advocated by European projects such as Unify [25] and 5GEx [1], with potentially significant influence on the definition of future 5G networks. ETSI also acknowledges the importance of an interface between an SDN controller and an NFV orchestrator,

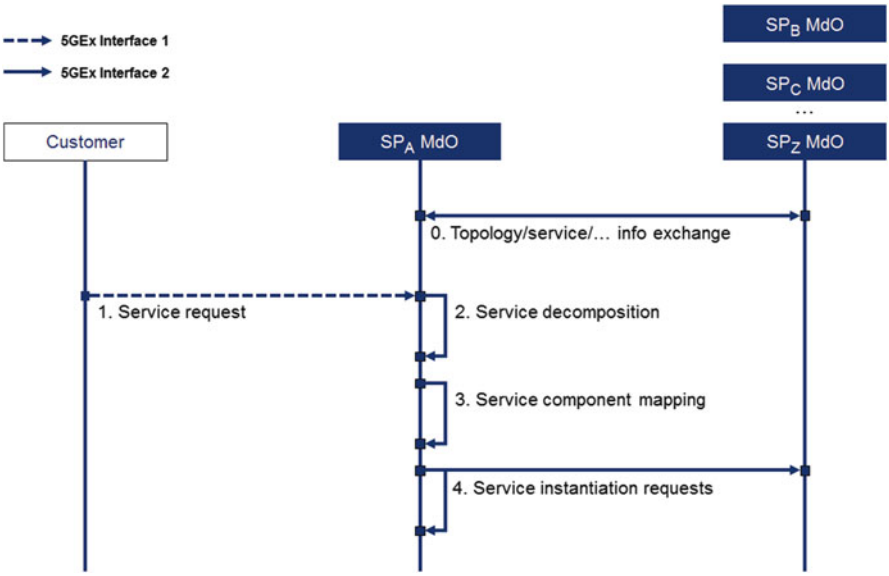

Fig. 10.5 Interactions subject to threats in a multi-provider scenario

being direct or indirect [10]. As an example of interaction, a controller should be able to push network decisions in the data plane using high-level requests generated by orchestrators. Conversely, an orchestrator should be able to receive network topology information from an SDN controller, possibly with a level of abstraction (e.g., hiding specific details of network devices). Moreover, ETSI states that topology information may be passed along in both directions [10].

The list of threats provided here is inspired by the study of ITU-T X.805 security architecture (Sect. 10.2.1). In addition, recent studies identifying attacks and vulnerabilities pertaining to the SDN/NFV domain are considered (e.g., [4, 6, 24]).

Potential threats for the scenario discussed in Sect. 10.3.1 are as follows:

- Destruction of information and/or other resources;
- Disclosure of information;
- Interruption of services;
- Loss of confidence in secure trading between service providers.

The above-mentioned list of threats is not exhaustive but covers a broad security spectrum for multi-operator networks as we discuss throughout this section. The following threat reasons will be taken into account in the discussions:

- Hijack the orchestrator or the SDN controller;
- Malicious/compromised applications;
- Configuration issues;

- Distributed denial of service (DDoS);
- Repudiation of shared data.

Orchestrator Hijacking and Service Interruption. An attacker that gains access to an orchestrator or SDN controller can disrupt any kind of communication within the network domain and affect inter-domain interactions for service delivery and provisioning. Specifically, cooperation between service providers can be affected due to packet loss or malicious forwarding behavior in the data plane. For instance, a service may require packets to be diverted to an ordered sequence of VNFs before reaching their final destination, a process known as service chaining. Such kind of forwarding behavior can be realized over the SDN paradigm, i.e., an SDN controller configures switches to apply a specific forwarding strategy to packets associated to a service. Thus, an attacker can interrupt the service by changing the forwarding behavior programmed at the SDN controller. It also holds for an MdO, since MdOs could interact with SDN controllers directly or indirectly.

SDN Controller Hijacking and Destruction of Information, Privacy Issues. Destruction of information is also a possible consequence of SDN controller hijacking. Data can be modified or corrupted as packets traverse the network, since SDN-enabled switches can be programmed to modify packet fields. Even though OpenFlow, the most noted SDN realization, mostly enables the controller to program the forwarding elements up to layer 4 in the stack, it is still possible to use SDN-enabled switches to modify any packet field (e.g., using P4[1] programs). Also, some types of applications running atop an SDN controller can be enabled to provide complete packet inspection and modification, possibly resulting in privacy issues due to disclosure of information encapsulated in data packets.

A question that arises from the above discussions is the method that makes it possible for an attacker to hijack orchestrators or SDN controllers. **Malicious applications** can be used for hijacking purposes [4]. Northbound applications atop an SDN controller or orchestrator should be provided with security features so that remote access is only performed by authorized entities. Any change in a resource state (e.g., forwarding element, database system, computational resource) should be restricted to trusted applications or monitored in real time. Also, controllers and orchestrators should have strong isolation properties to prevent applications from interfering with one another.

Configuration Issues and Disclosure of Information. Threat reasons are not restricted to malicious activities. In fact, misconfigurations in an orchestrated network can lead to serious threats such as disclosure of information. Configuration mistakes can lead the orchestrator to originate data without authorization. In addition, configuration issues can lead to mistaken or incorrect data sharing such

[1] http://p4.org/

Table 10.5 Summary of threats and their reasons

Threat	Reasons
Destruction of information and/or privacy issues	SDN controller hijacking Malicious/compromised applications
Disclosure of information	Orchestrator/SDN controller hijacking Configuration issues
Interruption of services	Distributed denial of service (DDoS) Orchestrator/SDN controller hijacking
Trading confidence between SPs	Repudiation of shared data

as the case in which an orchestrator exposes resources which the operator does not actually own.

Flooding, DDoS, and Interruption of Services. DDoS attacks in which multiple compromised hosts flood the network with packets are a notable form of service interruption. A large number of requests to an orchestrator such as service requests can prevent its functional modules from working properly. For example, services offered by an MdO can become unavailable in case advertisements of service catalog or resource topology are not performed as expected. In addition, a large number of coordinated packets that traverse the data plane can overload the SDN controller, requiring it to process too many packets for flow rule decisions which can lead to service disruption in the controller.

An important discussion is how an SDN controller and an orchestrator make the network more susceptible to DDoS in comparison with other networking paradigms. A centralized element for the control plane is the main reason for such vulnerability which also holds for an orchestrator. However, the control plane can be physically distributed, enabling the use of methods for controller placement to mitigate DDoS attacks. It is worth noting that distributed SDN controllers will have to perform synchronization in order to keep network state in a logically centralized fashion.

With respect to **repudiation of shared data**, an operator could claim to not have originated data units. Specifically, the operator could have agreed to share network resources but still denies such agreement or sharing. Non-repudiation issues can affect the confidence to encourage trading opportunities between service providers. A brief discussion on non-repudiation over ITU-T X.805 is provided in Sect. 10.2.1.

Table 10.5 presents an example of mapping threats and their reasons based on the discussions above

10.3.3 Security Schemes

Before reviewing potentially applicable security schemes and countermeasures, it is important to emphasize cryptographic protocol suites that provide basic services such as authentication and encryption. For example, Internet Protocol Security

Table 10.6 Potential security schemes and countermeasures

Threat Reason	Possible countermeasure
Orchestrator/SDN controller hijacking	Restrict malicious/compromised applications with application containerization
Configuration issues	Real-time policy checker
DDoS	Physically distributed SDN controllers; detect attack and redirect legitimate traffic to a new server address
Repudiation of shared data	Digital signatures over ITU-T X.509

(IPSec) provides end-to-end security in the IP layer. IPSec can be used to protect data flows between a pair of hosts, a pair of security gateways, or between a security gateway and a host. Another example is Transport Layer Security (TLS), which allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery [7]. TLS is designed in particular for communications over a reliable transport protocol such as TCP. A brief comparison between IPSec and TLS draws the attention to the fact that the latter protects application streams, while IPSec connects hosts to entire private networks, including across a public network.

Table 10.6 presents potential countermeasures against the threat reasons (thus, threats).

The impact of malicious application behavior can be restricted or prevented by using (or providing support to) application containerization [24]. Note that network applications can be statically compiled with the controller code or instantiated as a dynamic module with the controller software. Containerization allows for authenticating the application during setup, and controlling the application's access rights on the infrastructure. In addition, containerization can limit and isolate the resource usage for each application.

To detect disclosure of information caused by configuration issues, it is possible to use policy checker mechanisms such as the work in [18]. In an SDN network, the controller is aware of the network state because it is responsible for flow rule decision and creation. Thus, SDN allows the verification of correct forwarding behavior. A policy verification example is "traffic originated from hosts A and B should never leave the domain during working time." One of the major challenges in policy verification is the separation of different types of traffic using fine-grained policy checking, since the SDN controller can set forwarding rules based on network identifiers, and it has a limited view on the type of traffic, e.g., application identifiers. This can be improved by using external traffic classifiers and deep packet inspection mechanisms in the network. To perform policy checking in case of multiple controllers in the network, it is also important to synchronize the network-wide state among all distributed controllers.

Since centralization of control makes an SDN network more susceptible to DDoS attacks, the immediate solution is to physically distribute the control plane. Detecting DDoS is another possible countermeasure, having traffic volume as a

trigger for an SDN application that also blocks malicious traffic. For instance, the work in [19] provides the following method: a blocking application sits atop the SDN controller and establishes a secure channel with the server under protection against DDoS – the server can be an orchestrator or an MdO. The secure channel is used by the server to notify the blocking application in case of DDoS attacks, and subsequently, the blocking application safely provides the server with a new IP address at which the service should resume. As a result, legitimate traffic is redirected from the attacked server address to a new address. Another method to prevent DDoS attacks is to use rate limiters at the data plane to detect the abnormal traffic that goes beyond a threshold value.

10.3.4 Gaps

Mapping security requirements to existing solutions in the literature, including recommendations from standards, draws the attention to at least three important topics: trust, Path Computation Element confidentiality, and privacy between operators. We next discuss these gaps before providing final considerations and concluding this chapter.

Trust Relationships Between Operators. A certification authority (CA) allows trust relationships by building, maintaining, and revoking digital certificates. These processes can be used within any given NFV context [8]. Note that a certificate verifies that a public key is owned by a particular entity, but it does not imply the trustworthiness of the key owner. This and other aspects of trust should be taken into account when using public-key infrastructure (PKI).

Should PKI be used for trust, we refer to the ITU-T X.509 to address some of the security requirements. The ITU-T X.509 can be seen as a hierarchical trust model for authentication [15]. It defines a certification authority tree in which a certificate within a local community is signed by a CA that can be linked into this tree. Such a rigid hierarchical structure may not be aligned with NFV-specific trust goals, since trust is highly dynamic and trust measures can combine a variety of assurance elements that include identity, attribution, attestation, and non-repudiation [8]. Thus, as far as trust is concerned, a trust objective should be defined before considering the use of PKI over the recommendations of ITU-T X.509.

PCEP Confidentiality in Multi-Operator Networks. In the context of 5GEx, a candidate mechanism for establishing inter-NSP (Network Service Provider) connectivity is the combined usage of BGP-LS (Border Gateway Protocol-Link State) for abstracted topology dissemination at provider level and PCE (Path Computation Element) for the actual path computation and instantiation of connectivity. In the case of inter-domain path computation, the end-to-end inter-domain path is a concatenation of intra-domain path segments resulting from cascaded PCE-to-PCE cooperative communications. Definitely, the PCE architecture can be considered as de facto standard to effectively deploy TE in multi-domain

networks [22]. However, despite the authentication, authorization, and encryption mechanisms [20], confidentiality issues still might arise inherently due to the exchange of information on network resource availability (e.g., link bandwidth) aimed at the inter-domain LSP setup. In fact, the information exchanged in inter-PCE communications can be used in a malicious way. Although the inter-NSP topology exchanged by means of BGP-LS represents an abstract topology with aggregated TE metrics and values, confidential information (e.g., the amount of available bandwidth in a inter-provider link) may be inferred. In fact, a requester PCE is not forced to actually set up the returned path by triggering a signaling in the network. Thus, a malicious requester PCE might issue a sequence of bogus, although formally licit, computation requests to a PCE belonging to a different domain with the only purpose of processing the returned replies to infer network resource availability information in other domains. For instance, multiple requests with the same destination node and different values of requested bandwidth might be submitted to a PCE. Instead of establishing the path, the obtained replies with bandwidth availability can be used to derive possible bandwidth bottlenecks toward the specified destination. This represents a security weakness that might be exposed by a NSP for obtaining valuable advantages in terms of market share by leveraging on potential failures and weaknesses of concurrent providers. Such a misuse of the path computation services might prevent a beneficial cooperation among PCEs belonging to different NSPs and compromise the dynamic provision of end-to-end LSPs. In fact, a PCE might not have an interest in processing a request if it is arriving from a competitor provider or if some security threat is perceived that is likely to cause any operational or economic damage. Therefore, inter-PCE interactions could be extended with (1) malicious PCEP usage discovery techniques [13, 21] and (2) trust-based and incentive-compatible mechanisms to discourage the misuse of path computation services while stimulating effective interactions among PCEs [12, 14].

Privacy in Collaborative Service Delivery. Cross-domain orchestration of resources over multiple administrative domains enables collaborative service delivery, i.e., services can be realized via chaining (or sequence) of VNFs over domains of multiple operators. In this case, while a VNF runs on the infrastructure of one operator, policies can come from another operator, which motivates an operator to encrypt its traffic in order to hide business or technical strategies. The aforementioned example is only one out of many possible use cases for privacy in collaborative service delivery. For instance, user data traffic could also be impacted (see Fig. 10.6). Thus, there is a need for security mechanisms and standards for enabling private VNFs [5].

10.4 Research Challenges and Future Directions

Resource sharing in a multi-party service delivery requires, among other things, a flexible and programmable infrastructure. Such flexibility is a key enabler for efficient 5G services through network slices [3], adapting to service demands and meeting the requirements of emerging use cases.

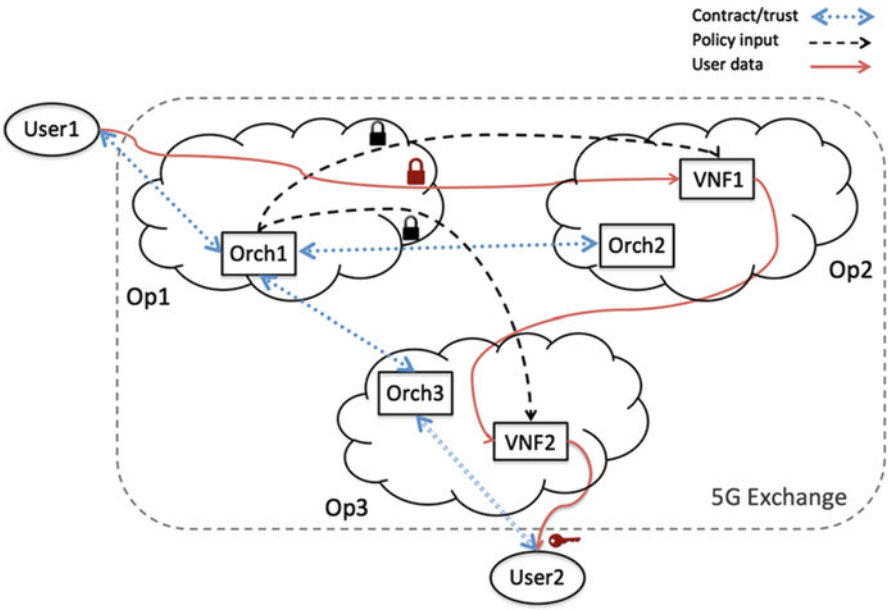

Fig. 10.6 Multi-operator service chaining and information flow [5]

In the context of security, network slices require strong isolation properties. Slices should not interfere with one another so that faults are not propagated through the network. Resilience and robustness are important in mission-critical business services such as public safety networks in which hierarchical SDN controllers can provide increased security features [23]. Other research challenges include trust, confidentiality, and evolved privacy solutions, as discussed in Sect. 10.3.4.

Multi-operator service orchestration and delivery in 5G bring intensified security concerns. This chapter has provided discussions on security requirements and threats related to service orchestration; moreover, potential solutions for securing 5G networks have been discussed. As operators want to be completely confident when hosting third-party service components in their infrastructures, such mapping of the threat landscape and threat mitigation strategies is essential. We argue that with the right design choices, future 5G networks will be able to meet the increasingly complex security requirements.

Questions

1. Explain how security dimensions can protect the management plane in multi-operator orchestration based on ITU-T X.805 standard?
2. Based on ITU-T X.805 standard, which security dimension can prevent the denial of authorized access to services in 5G?

3. What are possible interactions between Multi-domain Orchestrators (MdOs) that are subject to threats in a multi-provider scenario?
4. What are the main threats associated with orchestrator/SDN controller hijacking?
5. What are the security threats in deploying NFV in multi-operator 5G network based on the recommendations from ETSI NFV?
6. Explain the importance of topology validation for security of end-to-end slices in 5G?
7. Explain your rationale why it is important to deploy strong AAA mechanisms for virtualized services in 5G?
8. Describe how misconfigurations in network can lead to an attack against the orchestrator and controllers?
9. Describe how DDoS attacks can lead to service interruption in MdOs and what are the possible countermeasures to prevent it?
10. Explain your reasoning why it is difficult to establish trust relationship between multiple operators?
11. Describe some of the privacy challenges for orchestration between multiple operators?

Acknowledgements This work has been performed in the framework of the H2020-ICT-2014 project 5GEx (Grant Agreement no. 671636), which is partially funded by the European Commission. Gergely Biczók has been supported by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

1. 5GEx EU H2020-ICT-2014-2, http://www.5gex.eu/. Accessed 01 Dec 2016
2. 5G White Paper, NGMN Alliance (2015). https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf. Accessed 5 Apr 2017
3. 5G Systems, Ericsson White Paper (2017). https://www.ericsson.com/res/docs/whitepapers/wp-5g-systems.pdf. Accessed 5 Apr 2017
4. Akhunzada A et al (2015) Securing software defined networks: taxonomy, requirements, and open issues. IEEE Commun Mag 53(4):36–44
5. Biczók G et al (2016) Private VNFs for collaborative multi-operator service delivery: an architectural case. In: Network operations and management symposium, 2016 IEEE/IFIP. IEEE, pp 1249–1252
6. Dabbagh M, Hamdaoui B, Guizani M, Rayes A (2015) Software-defined networking security: pros and cons. IEEE Commun Mag 53(6):73–79
7. Dierks T, Rescorla E (2008) The transport layer security (TLS) protocol version 1.2. RFC 5246
8. ETSI (2014) NFV Security and Trust Guidance. Technical Report ETSI GS NFV-SEC003
9. ETSI (2014) NFV Security Problem Statement. Technical Report ETSI GS NFV-SEC001
10. ETSI (2015) Report on SDN usage in NFV architectural framework. Technical Report ETSI GS NFV-EVE 005
11. ETSI (2016) NFV MANO Report on Architectural Options. Technical Report ETSI GS NFV-IFA 009
12. Fung CJ et al (2014) Quality of interaction among path computation elements for trust-aware inter-provider cooperation. In: 2014 IEEE international conference on communications. IEEE, pp 677–682

13. Gharbaoui M, Paolucci F, Giorgetti A, Martini B, Castoldi P (2013) Effective statistical detection of smart confidentiality attacks in multi-domain networks. IEEE Trans Netw Serv Manag 10(4):383–397
14. Gharbaoui M et al (2016) An incentive-compatible and trust-aware multi-provider path computation element (PCE). Comput Netw 108:40–54
15. Grandison T, Sloman M (2000) A survey of trust in internet applications. IEEE Commun Surv Tutorials 3(4):2–16
16. Guerzoni R et al (2016) Analysis of end-to-end multi-domain management and orchestration frameworks for software defined infrastructures: an architectural survey. Trans Emerg Telecommun Technol 28(4):1–19. http://onlinelibrary.wiley.com/doi/10.1002/ett.3103/full
17. ITU-T (2003) Security architecture for systems providing end-to-end communications. X.805
18. Kazemian P et al (2013) Real time network policy checking using header space analysis. In: Presented as part of the 10th USENIX symposium on networked systems design and implementation, pp 99–111
19. Lim S, Ha J, Kim H, Kim Y, Yang S (2014) A SDN-oriented DDoS blocking scheme for botnet-based attacks. In: 2014 sixth international conference on ubiquitous and future networks. IEEE, pp 63–68
20. Lopez D, de Dios O, Wu W, Dhody D (2016) Secure transport for pcep. Internet-Draft draft-ietf-pce-pceps-10, IETF Secretariat, July (2016). http://www.ietf.org/internet-drafts/draft-ietf-pce-pceps-10.txt
21. Paolucci F, Gharbaoui M, Giorgetti A, Cugini F, Martini B, Valcarenghi L, Castoldi P (2011) Preserving confidentiality in PCE-based multi-domain networks. J Opt Commun Netw 3(5):465–474. art. no. 5759822
22. Paolucci F et al (2013) A survey on the path computation element (PCE) architecture. IEEE Commun Surv Tutorials 15(4):1819–1841
23. Santos MAS et al (2014) Decentralizing SDN's control plane. In: 39th annual IEEE conference on local computer networks. IEEE, pp 402–405
24. Scott-Hayward S, Natarajan S, Sezer S (2015) A survey of security in software defined networks. IEEE Commun Surv Tutorials 18(1):623–654
25. UNIFY EU FP7. http://www.fp7-unify.eu/. Accessed 01 Dec 2016

Mateus Augusto Silva Santos received his M.Sc (2009) in Computer Science and Ph.D. (2014) in Electrical Engineering from Universidade de São Paulo (USP), Brazil. From 2013 to 2014 he was a research scholar with the Inter-Networking Research Group at UC Santa Cruz. He was also a postdoctoral researcher with University of Campinas (UNICAMP). His research interests are in software-defined networking, network security and wireless networks. He has industry experience in the following organizations: Hewlett-Packard and EMBRAER. He is currently a researcher at Ericsson in Brazil.

Alireza Ranjbar received his M.Sc degree with distinction from Aalto university, Finland in the field of Communications Engineering in 2015. Currently, he is working as a researcher at Ericsson Research, Finland. His current research interests include Software-defined networks, Security, and Cloud computing.

Gergely Biczók is an assistant professor at the CrySyS Lab at the Budapest University of Technology of Economics, where he received his PhD in Computer Science in 2010. Previously, he was a postdoc at the Hungarian Academy of Sciences and the Norwegian University of Science and Technology, a Fulbright scholar at Northwestern University and a research fellow at Ericsson Research. His research interests center around the economics of networked system including security, privacy and 5G systems.

Barbara Martini after getting her degree in Electrical Engineering, she worked at Italtel first and later at Marconi Communications, in Italy. Since 2003 she has been a research engineer at the CNIT National Laboratory of Photonics Networks in Pisa, Italy and she is affiliated Researcher within TeCIP Institute of Scuola Superiore Sant'Anna. Her research interests include transport network management, GMPLS/SDN control and service architectures for next generation networks and clouds, orchestration in software-defined infrastructure. She has been involved in several research project funded by EU FP7 (NOBEL, NOBEL Phase 2, BONE, OFELIA, FED4FIRE, 5GEx). She authored more than 80 papers in scientific journals and international conference proceedings. She is a co-chair of the Workshop on Orchestration for Software-Defined Infrastructures (O4SDI) held at IEEE ICC2016 and NFV-SDN2016. She is currently serving as a TCP Member of several IEEE conferences (ITU Kaleidoscope, ONDM, IEVC, APNOMS, NETSOFT) and as reviewer for IEEE journals (JLT, JOCN, IEEE Network, TNSM). She is also involved in IEEE P1903 WG on Next-Generation Service Overlay Networks (NGSON), IETF NFV-related initiatives and IEEE SDN Standardization Committee.

Francesco Paolucci received the Laurea degree in Telecommunications Engineering in 2002 from the University of Pisa, Italy and the Ph.D. degree in 2009 from the Scuola Superiore Sant'Anna, Pisa, Italy. In 2008 he was granted a research Merit Scholarship at the Istitut National de le Recherche Scientifique (INRS), Montreal, Quebec, Canada. Currently, he is Assistant Professor at the TeCIP Institute of Scuola Superiore Sant'Anna, Pisa, Italy and Affiliate Researcher of CNIT, Italy. His main research interests are in the field of optical networks control plane, including Generalized Multi Protocol Label Switching (GMPLS) and Software Defined Networking (SDN) protocol extensions, impairment-aware routing based on Path Computation Element (PCE), inter-domain traffic engineering and flexible optical node architectures. Other research activities include network services for Grid/Cloud Computing applications, optical network fault tolerance, inter-domain security and confidentiality. He is co-author of one IETF Internet Draft, 4 international patents, more than 100 papers on international journals and conference proceedings. He has been involved in European research projects on next generation optical networks and innovative control and management of transport networks (BONE, NOBEL, STRONGEST, IDEALIST, PACE, 5GEx). He has served as Work Package Leader within the PACE Project (CSA).