Communication papers of the Federated Conference on Computer Science and Information Systems, pp. 127–130
DOI: 10.15439/2017F235
ISSN 2300-5963 ACSIS, Vol. 13

Trustworthiness 5G Enabler

Rafał Artych, Krzysztof Bocianiak, Tomasz Ośko
Orange Polska S.A.
R&D Center
ul. Obrzeżna 7, 02-691 Warszawa, Poland
Email: {rafal.artych, krzysztof.bocianiak, tomasz.osko}@orange.com

Abstract—**This paper introduces security enabler for 5G networks that can be applied to improve network's own security and utilized by network users in their own service protection methods. Its main role is to process technical information present in the network in order to provide trustworthiness information that can facilitate necessary trust decisions. Network Provided Trustworthiness system matching 5G architecture is proposed to provide this functionality.**

I. Introduction

5G is the proposed next generation of network technology envisaging a wide variety of actors and device types, more use of the cloud and virtualization techniques and built-in security and privacy protection [1][2][3]. In this paper the idea of using network information in managing trust relations within the 5G network and services offered over the network is discussed. This idea follows popular network assets exposition principle while retaining security and privacy protection requirements.

Among multiple novel technological approaches (needed for variety of services e.g. enhanced Mobile Broadband (eMBB), Ultra-Reliable Low Latency Communications (URLLC), massive Machine Type Communication (mMTC)) 5G envisages delegation of access control to 3rd party, new authentication methods and security enablers used on demand. The security enablers are expected to protect subscribers, devices and their communications but also the integrity of the network itself.

New security requirements arisen during ongoing process of specification and standardization of 5G networks include:

- proper tool support and automation in order to face growing system complexity that could go outside human control,
- exposition of information about each step of service delivery for the purpose of end to end security management and orchestration,
- awareness of all 5G system stakeholders of their technical security context based on evidences, facts, indicators and proofs collected at network infrastructure level,
- provision by 5G systems and components of functionality to mutually assess the trustworthiness before and during interactions.

Presented above requirements can be considerably fulfilled by trustworthiness assessment enabler discussed in this paper.

Software Defined Networking (SDN), Network Function Virtualization (NFV) and cloud computing technologies are expected to enhance the flexibility of network function provisioning and update, as well as reduce deployment and maintenance costs. However, security and trust become a crucial issue in practical deployment of these technologies in 5G due to lack of practical security and trust architecture that can support virtualized networks[4]. General approach that can cover trust assessment in access networks, virtualized core networks and user-network relation is proposed.

Between network users and external service providers (SP) trustworthiness assessment is close to IP reputation or anti-fraud solutions based on IP address geolocation. Industry-leading IP geolocation solutions provide multiple data points, including: connection type, time zone/language, proxies, ISP, connection speed, latitude/longitude, home/business, demographics, phone Area Code, industry codes, autonomous system number (ASN), etc. Having this information allows companies to adapt their policies of security, content presentation and encoding at a granular level. However, accuracy, reliability and scope of commercial IP geolocation services depend on the employed algorithms and methodologies. Since the providers are using proprietary methodologies the quality of delivered information can be regarded as questionable [5]. In contrary to external providers, network operator can provide information that is based on data directly available from 5G network. Moreover, network operators are legally obliged to collect and retain data needed for business operation and required by law enforcement agencies. These unique data can be used to gain added value from the network that differentiate operators from other players.

Novel 5G systems bring opportunity of developing new solutions for attack prevention, security and trust management [6]. Proposed approach can be integrated into

currently considered 5G architectures and help to combine privacy protection requirement with the need for detailed security monitoring. It can be further extended into context-based security by adding contextual information available directly from network core platforms and support systems (contextualization).

The remainder of this paper is structured as follows. Section 2 provides brief introduction to the notion of trustworthiness. In section 3 we describe Network Provided Trustworthiness system and section 4 gives more details about its operation in specific use cases. Finally in section 5 conclusions and future plans are presented.

II. Problem statement – trustworthiness

There is currently no defined standard for 5G and technical standardization work has just begun. The security considerations for 5G cover new trust models, where infrastructures are shared by multiple virtual mobile network providers, but also take into account novel technological approaches such as multi-tenancy, network slicing, network virtualization and other novel technologies. It is required to control the exposure surface to new types of threat specific to 5G networks and to provide proactive mechanisms to protect against them. Trust based mechanisms can be among possible solutions [7]. Therefore, notions of trust and trustworthiness need to be introduced.

Trust is a belief and is related to risk. A trust decision about given entity is then a decision to accept the risk that the entity will not act as expected [8]. Trustworthiness is a property of being reliable that could be measured objectively. Information on the trustworthiness of other entities is crucial in order to make correct trust decisions. The optimal situation is when trust in an entity and the trustworthiness of that entity are in balance. If trust in an entity is lower than its trustworthiness, the trustor will take additional precautions or limit the scope of the relation – as a result he will increase his costs or decrease his profits. If trust is higher than the trustworthiness of the entity, the trustor will be exposed to more risk than he expects, consequently he can suffer a loss [9].

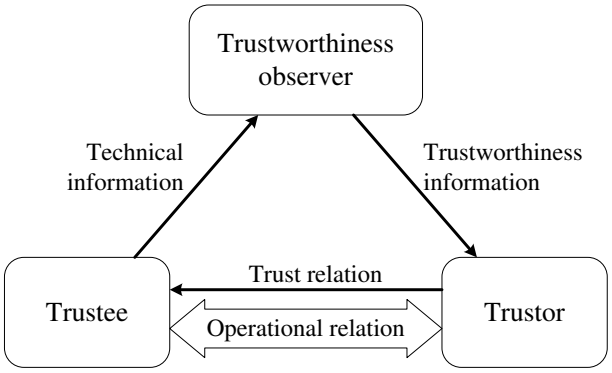

Fig. 1 Building trust relation using trustworthiness information delivered by Trustworthiness observer

Trustworthiness enabler that can be applied both to improve trust relation establishment within the network and to support external service providers in trust relation management with their customers is proposed in this paper.

While there are approaches to infer trust from comparison of observed metrics with expected values of given parameters, it is proposed to compute multi-dimensional trustworthiness level allowing direct interpretation. This computation is performed by dedicated entity having needed technical information from the network. The trustworthiness level is then used directly by trustor to build trust relation with trustee (cf. Fig.1). In this model the trustworthiness information is delivered to trustor while privacy of trustee is kept.

III. Enabler description

Proposed enabler should offer security context describing each connection that allows components of 5G system to take trust decisions. Moreover, it should support service providers in trust relation management with their customers. Referring to the model presented above the trustworthiness enabler plays the role of trustworthiness observer that gathers needed technical network information and exposes trustworthiness information.

In order to build the security context, relevant information needs to be collected at each segment of the network. When the connection is processed inside consecutive network segments the information included in the security context can be refined and extended. Finally it should be aggregated, correlated and propagated for future decisions regarding security, fraud prevention or characterization of risk.

In the 5G network architecture trustworthiness enabler functionality can be achieved with specialized subsystem distributed over the network. As depicted in Fig. 2 dedicated agents – Trustworthiness Watchers (TW) need to be placed in subsystems of 5G network, where information about connection is generated or processed. In the presented 5G ecosystem TW agents are located in network infrastructure (both physical and virtual), network functions and service layers both in access and core networks. Another set of information can be extracted from management systems and end to end (E2E) Orchestration layer.

Native network information received from TWs is aggregated and correlated by Network Provided Trustworthiness (NPT) system. The resultant trustworthiness information can be made available to network operator's service platforms or 3rd Party platforms offering services over the network in the form of security context. In considered here 5G architecture orchestrator can use security context of given connection to monitor required security level, but also to expose this information to 3rd parties.

Dynamic and programmable nature of 5G network allows not only computation of trustworthiness information but also negotiation and enforcement of required trustworthiness level.

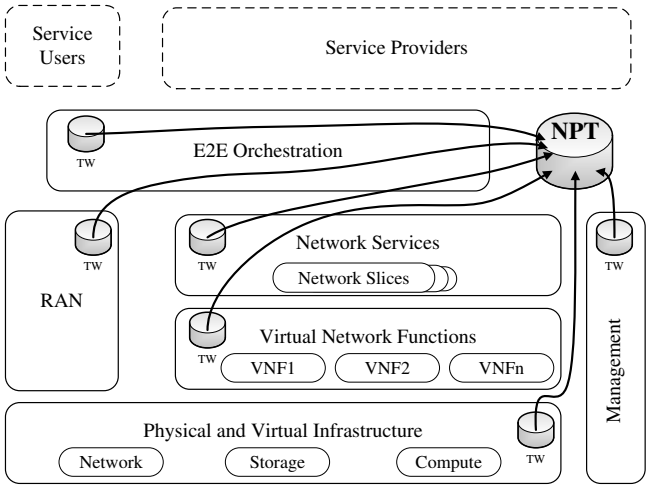

Fig. 2 NPT system within 5G ecosystem – logical view

The orchestrator can be seen as a key system of such solution where NPT system provides current security context of given connection. The user of that connection requires from the network to maintain current trustworthiness level or increase it according to needs. The orchestrator can then activate detailed monitoring of connection security metrics or change network configuration to fulfill user requirements.

In order to perform evaluation of given connection NPT system follows it inside the network, collecting metrics available in specified segment of the network. For example from Radio Access Network (RAN) the following information can be obtained: access type, location, location changes, radio link parameters, whereas the network Core segment can provide information on authentication scheme, service authorization, service parameters, associated resources. Finally, subscription parameters and its duration can be obtained from management systems.

The scope of security context in 5G network can include following areas:

• Customer's network context - encompassing the access network type, the equipment, the authentication scheme used, the device operating system and the equipment location;

• Infrastructure context – consisting of hardware and virtualization platforms' security parameters, attributes of VNFs (given function can be implemented using different software vendors - including open source software), network (physical and virtual) infrastructure security attributes including security policies, management capabilities and monitoring capabilities (telemetry, agents and probes);

• Customer relation context – covering parameters of contract and history of subscription.

The role of NPT system is to compute trustworthiness information from aggregated data (transform it into single value or vector of values) in order to facilitate trust decisions and hide details (customer privacy and network security principle). As trustworthiness is derived from technical context it does not cover all factors impacting the trust relation, nevertheless, this technical factor (beside human, social, formal and other factors) can play important role in trust establishment and risk management.

Service providers may be interested in more refined security context indicating directly risk of specific threats – in this case technical information from the network needs to be transformed into warning about possibility of specific attack types, for example: Man in the middle, Eavesdropping, Denial of service, Rogue devices, Data manipulation, Content piracy, Spoofing, Impersonation, Unprotected endpoint used for network entry, Equipment cloning, etc. (cf. [10]). The proposed enabler can bring into operation such functionality by extending its analytics to be compatible with this new security context.

IV. Use Cases

The usage of trustworthiness enabler can be illustrated by following examples.

A. Trust in network access control

Heterogeneity of access control to the network is one of considered 5G features [6] – it allows AAA (Authentication, Authorization and Accounting) function to be based on different authorization schemes and to be delivered by multiple providers. This approach implies the need to propagate the trustworthiness of the device accessing the network in the end to end relation. The NPT system can help to make the right trust decision to achieve required isolation and traffic segregation for devices using different access control configurations. Data about customer network context (access network type, equipment, authentication scheme and authentication provider) are discovered and transformed into trustworthiness information by NPT. Network service platforms can use this information in trust decisions about service level deciding about traffic priority and QoS (Quality of Service), fraud prevention monitoring, etc. For example specific security policy can be invoked for equipment authenticated within untrusted access network (indicated by low value trustworthiness information).

B. Trusted network slicing

Network slicing is often described as a technique that would help 5G network to implement variety of services with effective use of resources [11]. With NPT system the management of the slice with high-level security requirement can be made easier by indicating trustworthiness of each component from access and core network. Trustworthiness information computed by NPT reflects the security level of each component. The slice security policy can state that if this level is not high enough, the given (physical or real) component cannot be included in the slice. Using trustworthiness information the security level can be continuously monitored over the life time of the slice. In NFV based infrastructure NPT can be used to build E2E trust metrics that include information from a variety of monitoring and enforcement tools, including attestation, Intrusion Defense Systems (IDS), Network Domain Security (NDS) and software management of VNFs [12].

C. Service provider risk management

NPT system helps service providers using 5G network to manage the trust decisions and introduce proper risk management techniques for service requests received from the network. In this case the most helpful trustworthiness information would include possibility of specific threats within particular request coming from 5G network. Trustworthiness information used in service delivery should reflect the probability that the service request is initiated by the legitimate user in secure conditions in the rightful way. This probability is not static but corresponds to different parameters that can be easily identified by the network Operator.

Proposed here use case was demonstrated by the authors within the present convergent network ecosystem. In the proof of concept implementation so called Trust Level structured as shown in Table 1 was added to requests directed to exemplary service provider's website.

TABLE I.
EXAMPLE OF TRUSTWORTHINESS STRUCTURE

Trustworthiness Dimension	Network information covered
Access Type	Origin of the request seen by the network (access network, interconnected network, etc.)
Network Authentication	Strength and type of authentication used to access network services
Equipment	Type of equipment originating the request on network level including software version
Contract	Information about contract type (postpaid/prepaid) and its duration seen by CRM system

Trust Level information allowed SP to adapt its service logic and protection mechanisms to risk related with given service request (cf. [13]). For example after receiving tuple of trustworthiness values {v,x,y,z} the risk of using stolen credentials in given request has been estimated by SP. According to this estimation the trust decision has been taken to offer the requesting user limited number of available actions on his account or to require additional authorization to perform sensitive operation. This way SP can improve protection of his electronic service accessed from multiple networks and provide fine–grained authorization.

Implementation of trustworthiness enabler as NPT system in 5G network can be based on more detailed information about the request and should offer service users (customers and service providers) the functionality to monitor and proactively modify connection parameters (access network, routing, protection methods) in order to achieve required trustworthiness level. On the other hand thanks to only numerical value delivered to service providers the privacy of end users is not disclosed.

V. SUMMARY AND NEXT STEPS

5G is the proposed next generation of mobile wireless broadband technology. As with previous generations of mobile technology, security and privacy remain fundamental underlying requirements for mobile applications and services across devices that access wireless networks. Adoption of new paradigms like NFV and network slicing may further raise requirements aiming at properly securing such complex system. New trust models are one of responses to this demand. Introduction of trustworthiness enabler facilitates trust management on multiple layers of 5G architecture. Additionally, proposed enabler supports implementation of flexible security requirement: rather than enforcing user plane protection, the network may allow applications to select and dynamically adapt the way the user plane is protected [14].

Ongoing progress of 5G architecture shaping and standardization will enable more detailed design of NPT system compatible with this architecture. Beside definition how specific network information is used to calculate trustworthiness, further study of the concept should include exchange of trustworthiness information between 5G networks, cooperation with non-5G providers or other partners within network ecosystem. There is also a need for study of business model including liability of network operator to deliver trusted and qualified information to SP (security extension of Service Level Agreement between 5G network operator and vertical service providers).

REFERENCES

[1] Gupta, Akhil, and Rakesh Kumar Jha. "A survey of 5G network: Architecture and emerging technologies." *IEEE access* 3 (2015): 1206-1232. doi:10.1109/ACCESS.2015.2461602

[2] Next Generation Mobile Network Alliance, "5G White Paper", Version 1.0, Feb 17, 2015.

[3] 5G PPP Architecture Working Group, View on 5G Architecture Version 1.0, July 2016

[4] Yan, Zheng, Peng Zhang, and Athanasios V. Vasilakos. "A security and trust framework for virtualized networks and software-defined networking." *Security and communication networks* (2015). doi:10.1002/sec.1243

[5] Koch, Robert, et al. "Using Geolocation for the Strategic Preincident Preparation of an IT Forensics Analysis." *IEEE Systems Journal* 10.4 (2016): 1338-1349. doi: 10.1109/JSYST.2015.2389518

[6] Selander, Goran, et al. "5G-ENSURE: D2. 1 use cases." (2016).

[7] Wang, Dongxia, et al. "Towards robust and effective trust management for security: A survey." Trust, Security and Privacy in Computing and Communications (TrustCom), 2014. doi:10.1109/TrustCom.2014.65

[8] Mohammadi, Nazila Gol, et al. "Trustworthiness attributes and metrics for engineering trusted internet-based software systems." International Conference on Cloud Computing and Services Science. 2013. doi: 10.1007/978-3-319-11561-0_2

[9] Phillips, Stephen, et al. "5G-ENSURE: D2.2 Trust model (draft)."

[10] 5G Security – Making the Right Choice to Match your Needs (A SIMalliance 5GWG technical white paper) http://simalliance.org/wp-content/uploads/2016/02/5G-Security-%E2%80%93-Making-the-Right-Choice-to-Match-your-Needs.pdf

[11] Next Generation Mobile Network Alliance, "Description of Network Slicing Concept." *NGMN 5G P* 1 (2016).

[12] Manzalini, A., et al., Towards 5G Software-Defined Ecosystems. Technical Challenges, Business Sustainability and Policy Issues, IEEE SDN White Paper, http://sdn.ieee.org/publications

[13] Li, Min, et al. "Privacy-aware access control with trust management in web service." *World Wide Web* 14.4 (2011): 407-430. doi:10.1007/s11280-011-0114-8

[14] Horn, Günther, and Peter Schneider. "Towards 5G Security." (2015). http://resources.alcatel-lucent.com/asset/200292