NFV refers to the replacement of traditional specialised hardware devices with software that can be installed on standardised, off-the-shelf piece of hardware. ETSI work on NFV was initially set to address a requirement to define a list of base security requirements imposed by lawful interception in the NFV architecture.

by Gerald McQuaid and Domenico Raffaele Cione

LAWFUL INTERCEPTION IN VIRTUALIZED NETWORKS (Sept. 2017)

Gerald MCQUAID is Chairman of ETSI Technical Committee for Lawful Interception and attending ETSI TC CYBER and 3GPP SA3 LI since 2004. Member of the EU Data Retention Experts Group under the auspices of the European Commission.

Domenico Raffaele CIONE, Ericsson Strategic Product Manager for Regulatory Solutions, is active delegate in ETSI Technical Committees for Lawful Interception (LI) and Retained Data (RD) since 2003.

1. NFV for 5G

The next-generation of mobile networks beyond the 4G LTE mobile networks of today is identified with the term **5G** which ETSI is managing as a new technology to provide markedly increased operational performance, as well as superior user experience and better network energy efficiency (ref. http://www.etsi.org/technologies-clusters/technologies/5g). The basic performance criteria for 5G systems have been set by the International Telecommunications Union (ITU) in their IMT-2020 Recommendation (ref. http://www.itu.int/en/ITU-R/study-groups/rsg5/rwp5d/imt-2020/Pages/default.aspx). Specifically, ITU-R M.2083 [1] describes the overall usage scenarios for 5G systems in terms of Enhanced Mobile Broadband (to deal with hugely increased data volumes, overall data capacity and user density), Massive Machine-type Communications for the IoT (requiring low power consumption and low data rates for very large numbers of connected devices), Ultra-reliable and Low Latency Communications (to cater for safety-critical and mission critical applications).

The 3GPP is the mobile industry standards body most actively working on 5G standards to submit proposed specifications to the ITU to be part of the IMT-2020 standard. By the second half of 2017 the focus of 3GPP work will shift to Release 15, to deliver the first set of 5G standards - including new work as well as the maturing of the LTE-Advanced Pro specifications.

At ETSI level, most effort is on the Virtualization of the Network Function (NFV) as major key component technologies which will be integrated into future 5G systems. **NFV** refers to the replacement of traditional specialised hardware devices with software that can be installed on standardised, off-the-shelf piece of hardware. It's similar to how we load various software applications on a computer. For example, instead of having a phone sitting next to your computer, you could install software that would allow you to make phone calls from the computer - and get rid of the phone on your desk. Simply put, NFV is about changing specialised communications equipment into software, and allowing the operator to bring resources to where they need them most. This should result in increased flexibility and reduced cost.

The multitude of use cases behind 5G requires the flexibility that is enabled by NFV and by extension, the open source community. NFV is now a prerequisite for having the kind of network to be able to address the IoT workload for 5G. Furthermore, the time is now for operators to formulate their strategies to transition their core network towards NFV architecture in preparation for 5G in 2020.

2. NFV Security/LI challenges

NFV greatly amplifies existing security problems in terms of impact. The vulnerabilities may be similar to todays, but it does concentrate them in one place and increase the likelihood of a common mode failure. In many ways, it puts all our "security eggs in one basket". In traditional telecommunications equipment, a number of factors helped frustrate would be attackers e.g. physical security, proprietary software, hardware, installation and configuration, and a reduced ability to exploit any vulnerabilities. This doesn't mean older equipment is more secure, just harder to exploit.

NFV is primarily software based i.e. all the functions of a traditional telco "switch" is now run by a virtual network function (VNF) – not unlike a program on a PC. The various functions (VNF's) are managed by a Hypervisor. If this Hypervisor is compromised, there is little current defense to maintain integrity or confidentiality.

There are a number of sensitive functions that are of concern, significantly anything that requires encryption or isolation. Examples of these functions are authentication (key for sim card security), network defense, logging functions and above all **lawful interception (LI)**.

Given the fact that NFV provides for a more harmonised infrastructure set, across operators and countries, any vulnerability could have much greater impact, particularly where critical national infrastructure obligations apply.

At today only a few Regulatory or Government security entities have a current understanding of the risks, more will follow.

3. LI in NFV in ETSI

ETSI work on NFV was initially set to address a requirement to define a list of base security requirements imposed by lawful interception in the NFV architecture.

The first actions were made at ETSI TC CYBER level and have resulted into two standard documents: one at recommendation level, [2] **TR 103 308 v1.2.1,** and another at normative level, [3] **TS 103 487 v1.1.1,** and both ones are usable to identify the baseline security requirements for LI as sensitive function for NFV.

At today, most standardization activity on LI in the NFV interception domain is driven by the NFV SEC sub-group within the Industrial Specification Group (ISG). NFV SEC is driving the standardization activity on LI and RD features in the NFV interception domain in coordination with TC LI.

A first phase was dedicated to identify the security and architecture pre-conditions for the provision of LI in an NVF based network. **GS NFV-SEC 004** [7] was defined as a guidance on the LI requirements when deployed in the NFV context for provision of the points of interception (PoI's) for each of Intercept Related Information (IRI) and Content of Communication (CC) with respect to the handover requirements defined by ETSI TC LI.

Particular implementation relevance was identified for the PoI location attestation and LI undetectability requirements. Latest two years most ETSI work was focused to define a feasible NFV LI Architecture starting from identifying how the standard LI Reference model (ref. Figure 2 in [5] and Figures 1 in [6]) should apply and be mapped into the new CSP architecture defined by NFV (Figure 1, see ref. [4] for NFV architecture description). Figure 1 below shows the relevant LI functional entities (drawn at left side of picture) under modelling into the new CSP NFV context (drawn at right side of picture): Administrative Function (AF), Point of Interceptions (PoI's identified as IRI-IIF and CC-IFF) and the Internal Interfaces (INI1 also called X1, INI2 also called X2, INI3 also called X3).

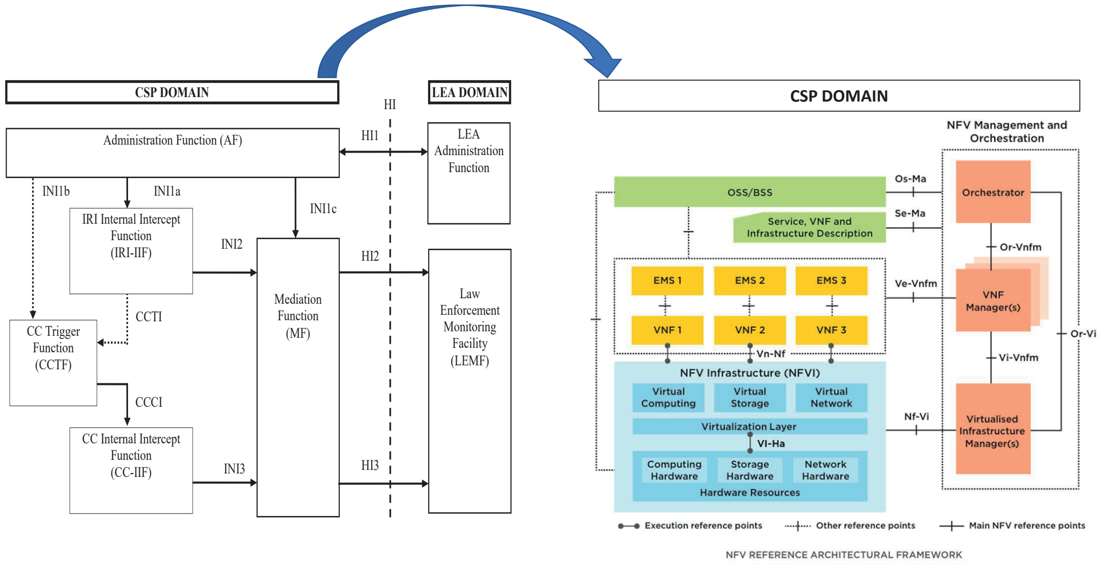
CSP DOMAIN
LEA DOMAIN
HI
Administration Function (AF)
HI1
LEA Administration Function
INI1b
INI1a
INI1c
IRI Internal Intercept Function (IRI-IIF)
INI2
HI2
Mediation Function (MF)
Law Enforcement Monitoring Facility (LEMF)
CCTI
CC Trigger Function (CCTF)
CCCI
CC Internal Intercept Function (CC-IIF)
INI3
HI3
CSP DOMAIN
NFV Management and Orchestration
OSS/BSS
Os-Ma
Orchestrator
Service, VNF and Infrastructure Description
Se-Ma
Or-Vnfm
EMS 1
EMS 2
EMS 3
Ve-Vnfm
VNF Manager(s)
VNF 1
VNF 2
VNF 3
Or-Vi
Vn-Nf
Vi-Vnfm
NFV Infrastructure (NFVI)
Virtual Computing
Virtual Storage
Virtual Network
Virtualization Layer
Nf-Vi
Virtualised Infrastructure Manager(s)
VI-Ha
Computing Hardware
Storage Hardware
Network Hardware
Hardware Resources
Execution reference points
Other reference points
Main NFV reference points
NFV REFERENCE ARCHITECTURAL FRAMEWORK

***Figure 1** - Mapping Standard LI Functional Entities into NFV Reference Architecture*

Main addressed issue was the secure configuration of the PoI when deployed as embedded or standalone VNF on top of a NFV infrastructure and how to keep it secure along the entire VNF lifecycle.

The results of this ETSI study has been formalizing into the definition of the new report **GR NFV-SEC 011** [8] which represents the most advanced description of the standard solution in NFV with reference to the Lawful Interception (LI) problem Statement, Architecture, Deployment scenarios. Furthermore, mainly based on the current needs from network operators which are requested just now to manage the CSP evolution from native legacy networks towards truly virtualized networks, the report has identified the relevant most probable evolution paths identifying appropriate intermediate steps and considering a LI solution for each path as well as the associated network challenges and solutions.

Coming ETSI NFV ISG work will be focused into the definition of a new normative specification on NFV LI (GS) also starting to solve detailed stage 3 aspects for LI. These work items will represent input towards 3GPP and ETSI TC LI whose activity will be addressed to finalize the definition of the LI internal interfaces (INI1 also called X1, INI2 also called X2, INI3 also called X3), the MF/DF structuring and the HI's possible impacts. ©

REFERENCES

[1] Rec. ITU-R M.2083 - Framework and overall objectives of the future development of IMT for 2020 and beyond (September 2015).

[2] ETSI TR 103 308 - CYBER; Security baseline regarding LI and RD for NFV and related platforms (v1.1.1 2016-01).

[3] ETSI TS 103 487 - CYBER; Security baseline regarding sensitive functions for NFV and related platforms (v1.1.1 2016-04).

[4] ETSI GS NFV 002 - Network Functions Virtualisation (NFV); Architectural Framework (v1.1.1 2013-10).

[5] ETSI TR 102 528 - Lawful Interception (LI) Interception domain Architecture for IP networks (v1.1.1 2006-10).

[6] ETSI TS 133 107 - Universal Mobile Telecommunications System (UMTS); LTE; 3G security; Lawful interception architecture and functions (3GPP TS 33.107 version 13.6.0 Release 13) (v13.6.0 2017-04).

[7] ETSI GS NFV-SEC 004 - Network Functions Virtualisation (NFV); NFV Security; Privacy and Regulation; Report on Lawful Interception Implications (v1.1.1 2015-09).

[8] ETSI GR NFV-SEC 011 Network Functions Virtualisation (NFV); NFV Security; Report on NFV LI Architecture (v.0.0.9B 2017-07).