ETSI GR F5G 010 V1.1.1 (2022-04)

GROUP REPORT

Fifth Generation Fixed Network (F5G); Security; Threat Vulnerability Risk Analysis and countermeasure recommendations for F5G

Disclaimer

The present document has been produced and approved by the Fifth Generation Fixed Network (F5G) ETSI Industry Specification Group (ISG) and represents the views of those members who participated in this ISG.
It does not necessarily represent the views of the entire ETSI membership.

Reference

DGR/F5G-0010Security

Keywords

F5G, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00   Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format at www.etsi.org/deliver.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

If you find a security vulnerability in the present document, please report it through our Coordinated Vulnerability Disclosure Program:
https://www.etsi.org/standards/coordinated-vulnerability-disclosure

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.
No recommendation as to products and services or vendors is made or should be implied.
No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.
In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Group Report (GR) has been produced by ETSI Industry Specification Group (ISG) Fifth Generation Fixed Network (F5G).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

1 Scope

The present document identifies security threats to F5G and recommends mitigation strategies against them where F5G is defined by its purpose and use cases [i.1] and its architecture [i.3]. The present document adopts the TVRA method defined in ETSI TS 102 165-1 [i.5].

NOTE 1: The identified mitigation strategies in the present document are outlined with respect to the risk analysis contained in the present document and are indicative in nature (i.e. are not fully specified). Some mitigations that are identified may require non-technical measures as part of the strategy and the present document identifies them.

NOTE 2: The worksheets from ETSI TS 102 165-1 [i.5] and cited in clauses 5, 6 and 7 are provided as an electronic attachment to the present document (see Annex A).

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI GR F5G 002: "Fifth Generation Fixed Network (F5G); F5G Use Cases Release #1".

[i.2] ETSI GR F5G 001: "Fifth Generation Fixed Network (F5G); F5G Generation Definition Release #1".

[i.3] ETSI GS F5G 004: "Fifth Generation Fixed Network (F5G); F5G Network Architecture".

[i.4] Common Vulnerability Enumeration (CVE®) list.

NOTE: Available at www.cve.org.

[i.5] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.6] Shannon Claude: "Communication Theory of Secrecy Systems". Bell System Technical Journal. 28 (4): 662. doi:10.1002/j.1538-7305.1949.tb00928.x.

[i.7] Kerckhoffs Auguste (January 1883): "La cryptographie militaire" [Military cryptography]. Journal des sciences militaires [Military Science Journal].

[i.8] M. Zafar Iqbal, H. Fathallah and N. Belhadj: "Optical fiber tapping: Methods and precautions", 8th International Conference on High-capacity Optical Networks and Emerging Technologies, 2011, pp. 164-168, doi: 10.1109/HONET.2011.6149809.

[i.9] Recommendation ITU-T X.800: "Security Architecture for Open Systems Interconnection for CCITT Applications".

[i.10] ISO 7498-2: "Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture".

NOTE: ISO 7498-2 and ITU-T X.800 contain the same text.

[i.11] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (GDPR).

[i.12] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive).

[i.13] Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC (Radio Equipment Directive (RED)).

[i.14] European Treaty Series No. 185: "Convention on Cybercrime".

[i.15] ETSI GR NFV-SEC 003: "Network Functions Virtualisation (NFV); NFV Security; Security and Trust Guidance".

[i.16] Recommendation ITU-T G.800: "Digital networks - General aspects. Unified functional architecture of transport networks".

[i.17] Recommendation ITU-T G.873.1: "Digital networks - Optical transport networks. Optical transport network: Linear protection".

[i.18] Recommendation IUT-T G.873.2: "Digital networks - Optical transport networks: ODUk shared ring protection".

[i.19] Recommendation ITU-T G.873.3: "Digital networks - Optical transport networks: Optical transport network - Shared mesh protection".

[i.20] National Vulnerability Database (NVD).

NOTE: Available at https://nvd.nist.gov.

[i.21] UK Computer Misuse Act 1990.

NOTE: Available at https://www.legislation.gov.uk/ukpga/1990/18/contents.

[i.22] ISO/IEC 15408-2: "Information technology - Security techniques - Evaluation Criteria for IT security - Part 2: Security functional components".

NOTE: Often referred to by the shorthand term "Common Criteria".

[i.23] TR-069: "CPE WAN Management Protocol".

NOTE: Available from https://www.broadband-forum.org/technical/download/TR-069_Amendment-6.pdf.

[i.24] IEC 60529: "Degrees of protection provided by enclosures (IP Code)".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI GR F5G 00 [i.1], ETSI GR F5G 001 [i.2], ETSI GS F5G 004 [i.3] and the following apply:

botnet: network of connected computing devices infected with malicious software and controlled as a group without the owners' knowledge

data packet jitter: absolute difference in arrival time between the fastest and the slowest data packet or voice frame with respect to end-to-end latency

EXAMPLE: An end-to-end connection has a transfer time determined in part by the physics of transmission and in part by the variable processing time required to perform analysis of headers. The variation in the transfer time between fastest and slowest is the jitter and is commonly absorbed in buffering across the network. Thus, if a packet can take between 100 ms and 1 500 ms to arrive it is often prudent to impose a buffer that is slightly longer than the maximum transit time and to feed data out of the buffer at a constant rate for the receiving application. The existence of a buffer adds a point of attack to the system by adding the buffer as a system asset.

end-to-end latency: time it takes to transfer a given piece of information from a source to a destination, measured at the application level, from the moment it is transmitted by the source to the moment it is received at the destination

trust: confidence in the integrity of an entity for reliance on that entity to fulfil specific responsibilities

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI GR F5G 002 [i.1], ETSI GR F5G 001 [i.2], ETSI GS F5G 004 [i.3] and the following apply:

AggN	Aggregation Network
AI	Artificial Intelligence
AN	Access Network
BNG	Broadband Network Gateway
CE	Customer Equipment
CPE	Customer Premises Equipment
CPN	Customer Premises Network
CVE	Common Vulnerability Enumeration
DC	Data Centre
EU	European Union
E-CPE	Edge CPE
FFC	Full Fibre Connection
GRE	Guaranteed Reliable Experience
LAN	Local Area Network
M&C	Management and Control
NVD	National Vulnerability Database
OLT	Optical Line Terminal
ONU	Optical Network Unit
ONT	Optical Network Terminal
OSI	Open Systems Interconnection
OTN	Optical Transport Network
PE	Provider Edge-Router
PPPoE	Point to Point Protocol over Ethernet
QoE	Quality of Experience
RG	Residential Gateway
SAP	Service Access Point
SMP	Service Mapping Point
SPP	Service Processing Point
VXLAN	Virtual Extensible LAN

4 Introduction to security review of F5G

4.1 F5G purpose and architecture review

The F5G network architecture is developed based on evolution of the current generation and deployment of fixed networks and focusses on the provision of more fibre connections, addressed using the term Full Fibre Connection (FFC), with high quality user experience, addressed using the term Guaranteed Reliable Experience (GRE). Thus for the purposes of the present document the core of the analysis is with respect to FCC.

The examination of use cases in ETSI GR F5G 002 [i.1] to drive the core set of F5G requirements identify a need for more data throughput and more control of uncertainties in that throughput. Thus, objectives including maximizing availability, minimizing end-to-end latency and minimizing data packet jitter (variation in packet arrival time), are all stated either explicitly or implicitly.

EXAMPLE: High end-to-end latency has a negative impact on real time operations across a network. High data packet jitter rates (variation in packet arrival time) require buffering of data to "smooth" the data delivery to applications.

Figure 4.2-1 from ETSI GS F5G 004 [i.3] describes the planar architecture and that is mapped, in part, to user expectations described in ETSI GR F5G 002 [i.1]. The intent of F5G is to enable more bits per second to the customer by exploiting Optical Transport Network (OTN) technologies and advances in local wireless networking, e.g. WiFi-6, resulting in each of FCC and GRE. The physical nature of all optical fibre transmission is that it is immune to ElectroMagnetic Interference (EMI), and the content of communication on the fibre is therefore not observable without direct access to the fibre. If, in addition, full optical switching is used there are no electrical signals directly in the signal/data path. It is known that optical fibres can be "tapped" and [i.8] summarizes a number of means of doing so. In some implementations switching of optical links includes devices that are susceptible to EMI and this is considered in the analysis.

NOTE 1: Whilst there may be elements of the customer premises network that maintain conventional copper wire based technology such technologies are not in the innovation sphere of F5G and are not directly addressed in the present document.

The managed security of optical networks is broadly addressed by the following services as defined by the OSI 7-layer security model (see Table 2 of Recommendation ITU-T X.800 [i.9] and its mirror ISO 7498-2 [i.10]):

- At layer 1: Connection confidentiality, Traffic flow confidentiality.
- At layer 2: Connection confidentiality, Connectionless confidentiality.
- At layer 3: Peer entity authentication, Data origin authentication, Access control service, Connection confidentiality, Connectionless confidentiality, Traffic flow confidentiality, Connection integrity without recovery, Connectionless integrity.

In addition the models of protection of the physical layer defined in Recommendations ITU-T G.873 series [i.17], [i.18] and [i.19] are taken into account that address some aspects of resilience in network provision (i.e. address the availability aspects of the CIA paradigm).

At higher layers the full suite of services described in Recommendation ITU-X.800 [i.9] apply. For the purposes of the present document only the lower layers of the OSI model are considered and only with respect to achieving FCC and GRE. The threat model addresses attacks against the Confidentiality, Integrity and Availability (CIA) of the assets in the system. Specific stakeholders are considered as targets of the attack on the system.

NOTE 2: The term availability in the CIA paradigm is intended to address many aspects of assuring the service or network is available to the right person at the right time thus includes aspects of identification, authentication and authorization.

4.2 F5G specificities

As indicated in clause 4.1 the purpose of F5G is to promote FCC and GRE. The architecture manages this by conceptualizing the network into 3 planes as shown in Figure 4.2-1.

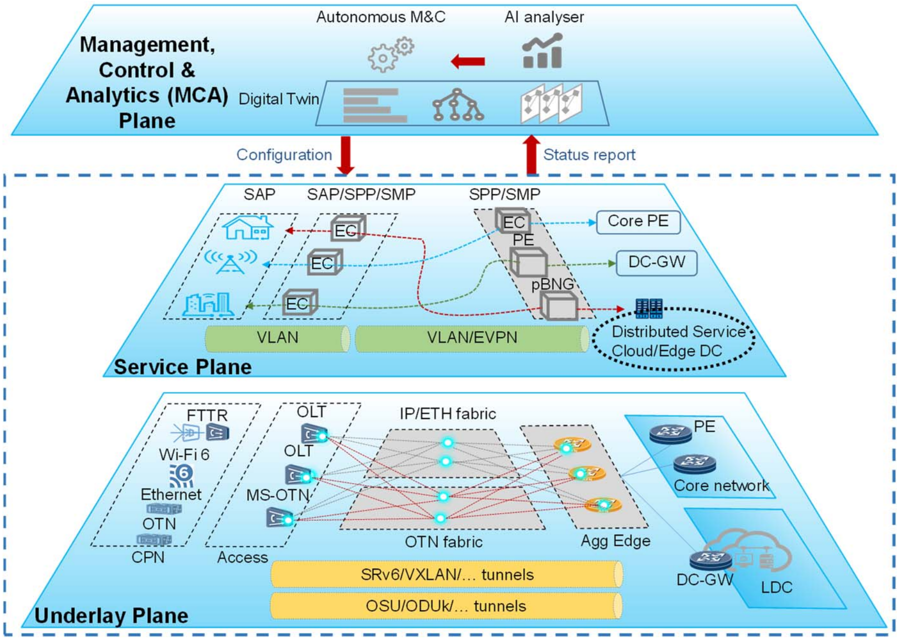

Figure 4.2-1: F5G network architecture

The F5G network architecture as shown in Figure 4.2-1 is comprised of 3 planes, an Underlay Plane, a Service Plane and a Management, Control & Analytics Plane (MCA Plane) with the following defining characteristics:

- Underlay Plane:
  - Carries the physical bits optically or electrically (OTN switches and Ethernet/IP switches and routers).
  - The Underlay Plane is comprised of physical network devices within 4 network segments:
    - Customer Premises Network (CPN);
    - Access Network (AN);
    - Aggregation Network;
    - Core Network.
  - Transmission technologies of the Underlay Plane are bounded (i.e. there are technology boundaries between network segments, which may be complemented by administrative boundaries in the Underlay Plane).

NOTE 1: Only the underlay plane can be defined as optical in nature, all other planes act on data and signalling without any fixed physical representation.

NOTE 2: Boundaries may be realized as interfaces in some instances and may implement some of the physical resilience measures identified in each of Recommendation ITU-G.800 [i.16] and in Recommendation ITU-T G.873 series [i.17], [i.18] and [i.19].

- Service Plane:
  - This plane provides service connections for customer and broadband service and is decoupled from the Underlay Plane. Service connections on the Service Plane can be dynamically created when triggered by protocols, e.g. Point to Point Protocol over Ethernet (PPPoE), or configured from the Management, Control & Analytics (MCA) Plane.

- Management, Control & Analytics Plane (MCA Plane):
    - The MCA Plane is in charge of management, control and performance analysis of the complete network. It is comprised of three logical components:
        - **Digital Twin**: models the network and defines resources, configuration and running models by real time analysis of network data to provide a real time model of the status and configuration of the network, which is the input for autonomous operation and artificial intelligence analysis (analysis is performed on the Digital Twin, not on the running model).
        - **Autonomous Management and Control** which is the main function for network configuration, service deployment, and network operation and includes the Intent Engine (a variant of natural language processing to derive intent from the user interface) and Autonomous Engine (enables MCA without direct human intervention).
        - **AI analyser**: analysis network data, identifies, locates and predicts network failures, provides management tools for QoE and analysing tools for network performance. It includes the Analysing Engine (realizes identification and analysis of network failures and drives close loop control of Autonomous Engine) and the AI Engine (performs data analysis and reasoning, in order to realize prediction of network failure and usage, and also failure identification and analysis).

The layering concept of Figure 4.2-1 is consistent with the OSI model of layering and the wider concept of information hiding using layers (or planes). One of the roles or purposes of the OSI model is to ensure that if a technology in the lower layers is evolved, e.g. the adoption of photons on optical transmission as opposed to electrons over copper wire transmission, the services that can be offered do not need to be changed.

EXAMPLE: A web service operates in the same way irrespective of the communication technology used from the client equipment to the core network (notwithstanding that a service designer may make presentation specialisations for the client device's screen, audio or user interface).

4.3 Network topology, network functions, and reference points

The F5G network provides connectivity, and high-speed, and high-quality, network services for subscribers. Figure 4.3-1 shows the F5G network topology with reference points T/T', U/U', V/Vo and A10/A10' which is a simplified version of the figure from ETSI GS F5G 004 [i.3].

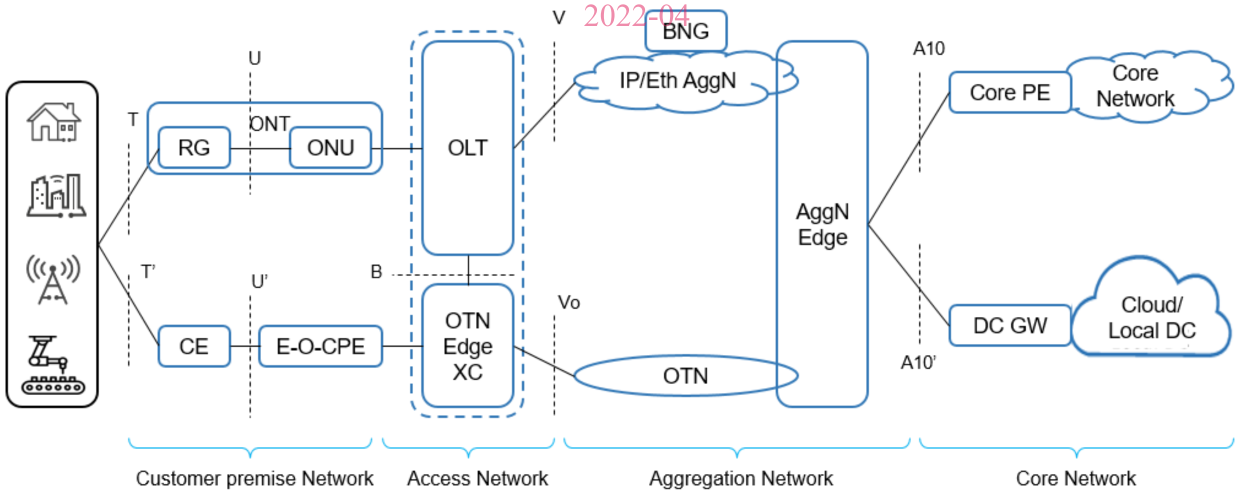

Figure 4.3-1: F5G network topology

In the case of premium private line, an OTN edge Customer Premises Equipment (O-E-CPE) represents the device that communicates with the OTN edge cross-connect on the network side, it is also the aggregation device for enterprise data. The enterprise network labelled Customer Equipment in Figure 4.3-1 and the Access Network is demarcated by the U' interface. The Optical Line Terminal (OLT) module in Figure 4.3-1 represents the data plane function of OLT and OTN edge cross-connect, the control and management function of OLT is not shown.

A Broadband Network Gateway (BNG) is a typical device in IP/Ethernet based Aggregation Network, which may be directly connected to an OLT or via an IP/Ethernet Aggregation network. A BNG may be implemented as a pool of devices although the pool represents a single function from the point of the present document. In some networks, there may be an IP aggregation network between the BNG and the Core Network. Besides typical IP/Ethernet aggregation network, OTN is also a possible option as complementary to typical IP/Ethernet aggregation. The OTN edge cross-connect aggregates the Access OTN traffic and will be a node on the OTN Aggregation Network. The Aggregation Network Edge represents the handover device between Aggregation Network and Core Network. It needs to identify and direct the traffic in both directions.

For the core network, considering local Data Centre (DC) and cloud service are getting more and more popular, it is an extension that expands the legacy core network. Even though the core network is not in the scope of the present document, the interfaces between Aggregation Network and Core Network need to be specified in the present document:

- The T interface is the handover point between adaptation box / E-CPE and the customer devices.
- The T' interface is the handover point between the CE and the enterprise devices.
- The V interface is the legacy IP/Ethernet based handover points between the Access Network and the Aggregation Network.

NOTE 1: It is anticipated that this interface will be improved in order to support new services.

- The B interface is the handover point between the OLT and the OTN edge cross connect.
- The Vo interface is the handover point between Access Network and OTN based Aggregation Network.

NOTE 2: For different services, the system may be configured to allow the OLT to handover the traffic via the V interface or the Vo interface.

- The A10 interface is the handover point between the Aggregation Network and the Core Network.

NOTE 3: In order to support new use cases in F5G, the A10 interface will be enhanced. The A10 interface is primarily Ethernet based, however, depending on reach, OTN may be used as the Ethernet transparent transport layer.

- The A10' interface is the handover point between the Aggregation Network and the Cloud or local DC.

For the purposes of the present document the system is bounded by the scope of each reference point and each reference point is assessed independently, and then in combination, to determine the overall system risk. The end-points of F5G are assessed as:

- Reference point T: user access point at which user's devices is identified, authenticated and connected to the Internet Services Provider (ISP) network.
- Reference point A10: the edge of ISP network where user's data is transmitted to the core network.
- Reference point A10': the edge of ISP network where user's data is transmitted to the local DC's.

The F5G network provides the following service to subscribers:

- Provide the access point for user's devices to connect to the carrier's network and from there to the services offered by the carrier, including access to the public Internet.
- Provide high-capacity, high-speed and high-quality, data aggregation and transporting services.

4.4 F5G security boundary and security objectives

As a working example of F5G the following scenarios apply:

- User's device connects to the Residential Gateway (RG) at reference point T, connects to the Optical Network Unit (ONU) at reference point U, connects either to IP/Eth AggN at reference point V or to OTN at reference point Vo, connects to the Core Network or Cloud/Local DC at reference point A10 or A10'.

- RG and ONU co-exist in the Customer Premise Network (reference point T faces user's devices, reference point U faces the Access network).

NOTE 1: The RG and ONU can be integrated as a single device named ONT or Home Gateway.

- OLT and OTN Edge XC co-exist in the Access network (reference point V faces the IP/Eth AggN and reference point Vo faces the OTN).

Each interconnecting device or service should only connect to peers with known and verifiable identifiers and thus build a trusted framework of network entities.

Dividing the security problem into a set of domains is a common approach and is offered below. It should be applied with care as there is a danger to consider domains in isolation and to forget, or to overlook, the inter-connectivity of these domains, and the use of one domain to attack another. It is also recognized that security design requires compartmentation such that a problem in one domain (compartment) can be isolated such that it does not impact another compartment (domain). Another design guideline is to simplify assumptions regarding the attacker, summarized by both Kerckhoff and Shannon:

- **Kerckhoff's principle [**i.7**]**: A cryptosystem should be secure even if everything about the system, except the key, is public knowledge.

- **Shannon's restatement [**i.6**]**: "the enemy knows the system", i.e. "one ought to design systems under the assumption that the enemy will immediately gain full familiarity with them".

The security objectives of each network domain in CIA(AA) paradigm are summarized below:

NOTE 2: The conventional Confidentiality, Integrity, Availability paradigm (the CIA paradigm) has been extended for greater clarification in ETSI TS 102 165-1 [i.5] as the CIAAA paradigm by the expansion of the "Availability" element to explicitly draw out the concepts of Authenticity (as a pre-requisite in access control) and Accountability (as a pre-requisite in integrity).

Table 4.4-1 provides a mapping of the security objectives and the threats defined in ETSI TS 102 165-1 [i.5].

Table 4.4-1: Threats to security objective types (from ETSI TS 102 165-1)

Threat	Objective type				
	Confidentiality	**Integrity**	**Availability**	**Authenticity**	**Accountability**
Interception (eavesdropping)	X				
Unauthorized access	X	X		X	X
Masquerade	X	X		X	X
Forgery		X	X	X	X
Loss or corruption of information		X	X		
Repudiation		X		X	X
Denial of service			X		

4.5 F5G stakeholder model

In order to assess the potential attacks it is essential to identify the stakeholders in the technology and services. A perfunctory analysis suggests the stakeholders include the manufacturers of equipment used in the F5G installations, the operators of services, the regulators of service, the direct customers or users of F5G (i.e. those offering traffic to the network), and indirect stakeholders who require access to knowledge, data or content of the network. The specific set of stakeholders is use case specific but for the purposes of the present document the simplified list above is used.

Several regulatory frameworks apply to any installation of F5G based systems and this includes the following (this list is indicative and no claim is made for its completeness in any market):

- General Data Protection Regulation (GDPR) defined in Regulation (EU) 2016/679 [i.11] and equivalent regulations in non-EU markets.

- Network Information Systems directive (NIS) defined in Directive (EU) 2016/1148 [i.12] and equivalent regulations in non-EU markets.