ETSI White Paper No. 62

A Vision for Communications Security

1st edition – May-2024

Authors:

Charles Brookson, Laurence Wayne, Scott Cadzow, Faraz Naim

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org

About the authors

Charles Brookson OBE CEng FIET FRSA

Director Zeata Security Ltd, Azenby Ltd

Charles worked in the Department for Business, Innovation and Skills of the United Kingdom Government for twelve years and is a Professional Electronic Engineer. He previously was Head of Security for the UK mobile operator one2one and worked in British Telecom for twenty years before that, in the last few years in the Chairman's Office. He has worked in many security areas over the last 40 years, including Cryptographic systems, secure designs, policies, auditing, and mobile radio.

He was Chairman on the GSM Association Security Group for 25 years. He worked within GSM and 3GPP security standards, first chairing the Algorithm Expert Group way in 1986, which helped define GSM Security. He was also involved helping to define Public Key Standards and ISO 27000 Standards. He was the first Chairman of the ETSI OCG Security, TC CYBER, and after four years the Vice Chairman. He was awarded an OBE for services to Telecommunications Security in 2015. He now is involved in various Companies.

Laurence Wayne MSc BSc

BT Group Plc (UK)

Laurence joined BT Group Plc as a data scientist in the Cyber Security arm of the business after completion of higher education at Durham University, consisting of an undergraduate degree in geophysics & geology, then a masters in scientific computing & data analysis. Recently, becoming involved in various Standards boards across ETSI and 3GPP, he has been enabled a unique insight into the cutting edge of cybersecurity - becoming rapporteur for this document in TC CYBER on laying the groundwork for 6G. This is his first official contribution to the standards community; and feels immensely privileged to be learning from & working alongside those with a wealth of experience and knowledge in this area.

Scott Cadzow

Cadzow Communications

Scott (ETSI Fellow 2023) is a passionate contributor to, and supporter of the role of standards in making more secure and more open products and services. In this respect Scott is rapporteur of a number of standards in ETSI TC CYBER and holds officer roles in a number of ETSI bodies including SAI, ETI, ITS and eHEALTH.

Faraz Naim B. Tech ECE

Accenture (UK)

Faraz is a part of Accenture UK and having 15 years of experience in Core Networks telecommunication with different technologies - CS, IMS, VoLTE, VoWiFi, M2M, IoT, 5G (SA/NSA), eSIM, Network Functions Virtualization (NFV) and IN-prepaid with multi vendors Telecom hands-on experience. He also supported MNO in the UK for TSA (Telecom Security Act). He has led multiple engagements across various clients in the Telecom Space across Asia, Europe, and Africa. He was also involved in ETSI ISG MEC and OCG AN for different activities. His contributions as a co-author for various white papers publication with ETSI are- (WP-49, WP-46_2nd Edition, WP-55, and WP-56). It's a great privilege and learning for him to work with the other co-authors of this white paper.

Contents

Executive Summary

This white paper presents a vision for the future of network security standardization and design, emphasizing the need for an Intelligent Trusted Network (ITN) to support the diverse and expanding array of communication technologies, including 4G, 5G, 6G and satellite systems. The proposed 6G network aims to provide universal access to digital services and voice, leveraging AI to support a wide range of devices and services. It will serve as a "Network of Networks", integrating existing and new infrastructures to maximize wireless connectivity.

The envisioned overlay ITN aims to provide comprehensive communication services, securing endpoints and users while utilizing the capabilities of future network environments. It introduces a Zero Trust security model, allowing secure interactions with end devices without relying on the security protocols of other networks. This network can be managed by various operators, each with their own security and trust frameworks. A significant aspect of this vision is the prevention of cyber-attacks through an understanding of new attack vectors specific to 6G.

Security requirements in fact, will vary significantly depending on the service; from simple temperature readings to sensitive personal health data, necessitating different levels of bandwidth, latency and packet loss. This paper acknowledges the challenges of securing legacy protocols like TCP/IP and SS7, which are integral to current networks but have known vulnerabilities. The ITN's overlay network is expected to enhance security despite these challenges.

Transition to 6G is described as evolutionary, building on existing networks, and revolutionary, with the introduction of the ITN. The agility of the network will be further improved by adopting open hardware and Open-RAN technologies. While the focus remains on completing the final phase of 5G until 2025, plans for 6G are underway, with promises for both consumer and business applications already being made. A strong emphasis must also be made regarding the environmental sustainability of the 6G network.

Context

The purpose of this white paper is to provide a vision to guide the security standardisation and design for future networks.

There are many communication options that can only grow in the future; 4G, 5G and 6G (from 3GPP), Internet of Things (IoT) (as enabled via LoRa[1], for example), local networks such as Zigbee[2] or Z-Wave, satellite systems and telecommunications. These will only grow more numerous and diverse.

Looking at the security requirements that are perceived for 6G: The purpose of 6G should be the enablement of effective access, by all people across the world, to digital services and voice. Also, that a novel Intelligent (possibly AI-enabled) trusted network should be the key feature of 6G which facilitates access to multiple access technologies including existing 2G-5G, plus the new 6G radio, as well as LEO[3] satellite and Wi-Fi[4] - whilst also catering for use via Private Networks.

In effect, with its overarching Intelligent Trusted Network (ITN), 6G would be one of the "Network of Networks", maximising access to wireless connectivity, leveraging all existing infrastructures as well as new ones.

One may start with the overarching purpose of 6G being the enablement of widest possible access, both by all people across the world and digital services including those provided by "things" (such as IoT devices, robots, drones, autonomous vehicles, virtual reality devices and similar). This also may be provided or supported increasingly by AI (voice taken for granted). This then arrives at 6G being a "facility" which will have been developed for multiple different business purposes. An appreciation that the requirements for each of these services will need to be different (i.e. bandwidth, latency, packet loss, etc) is needed, and that without a new network, these will rely on technology that may be dated or insecure. For example, the security requirement for a temperature probe reporting a reading every 15 minutes will be different from sending personal health data.

Most of these current networks must support legacy systems for security (such as authentication, identity, and privacy), typically utilising existing protocols over 40 years old such as TCP/IP and Signaling System Number 7 (SS7). It will likely be necessary to include these protocols, in some regard at least, in 6G; however there should be an awareness that they are very difficult to secure effectively and already have numerous known weaknesses. This means they cannot be wholly relied upon to serve the new network effectively, without inherently being vulnerable. Their combination with an Intelligent Trusted Network, however, should enable a greater level of security.

Leveraging existing networks is evolutionary, yet the aforementioned idea of an Intelligent Trusted Network is revolutionary. The added benefit of this new network is increased agility from the option of using open hardware and Open-RAN, including open interfaces in the hardware.

Both consumer and business promises are already being made for 6G, however releasing the final phase of 5G remains the priority until 2025 - with 3GPP only just beginning to plan 6G as a viable technology.

[1] https://lora-alliance.org/
[2] Zigbee is an IEEE 802.15.4-based specification.
[3] A Low Earth Orbit (LEO) is one where the period around the Earth is less than 120 minutes.
[4] A family of protocols based on IEEE 802.11

Therefore, a great deal of uncertainty still exists around the specifics of how the network will operate, compared to what has come before - currently most 5G networks revert to a trusted 4G network; likely resulting in the conceptual jump from 5G to 6G being substantial. This means the specifics of the 6G network will likely not be understood in any detail until this planning phase is well under way.

There are now many legislative requirements to ensure the security of communications, such as in the UK The Telecommunications (Security) Act 2021[5], the Product Security and Telecommunications Infrastructure Bill[6], and European requirements, outlined in the ENISA 5G Cybersecurity Standards report[7].

This white paper is a 'requirements recipe' to aid the building of a secure network. Prioritisation of the requirements should be discussed and realised further.

The vision of an overlay trust network that can securely connect endpoints to a secure trusted network seems to be the best way of handling all these perceived security requirements, threats and risks.

Vision

The vision is to have an overlay trusted network, that has all the properties required to manage and provide communications services, using the rich environment of other networks that will exist in the future. This aims to secure endpoints and users, in order to present a managed risk profile to endpoints and users. Whilst the vision is of an overlay trusted network, the question still remains of how endpoints authenticate to each other, and how critical infrastructure-discovery services are authenticated. Trust and risk are somewhat interconnected: A trusted entity should offer a greater degree of integration to a user's risk profile than an untrusted entity, or alternatively if an entity cannot be trusted it presents an unquantifiable level of risk.

This "***Network of Networks***" is used in our security vision to impose a Zero Trust regime[8] of security and management to other networks and communicate securely with end devices or users (see Figure One).

This is to allow the use of other networks, without depending on their security, maturity in the market, business models, or trust models. The trusted network provides a method of secure communication to talk to the other networks.

The trusted network can be used and operated by an Operator, Virtual Operator, Business, Private Operator or anyone who wants to connect to end devices wherever they are connected. It can be virtual or exist in hardware. These operators will have their security, trust models and requirements.

[5] https://www.legislation.gov.uk/ukpga/2021/31/enacted

[6] https://www.gov.uk/government/publications/product-security-and-telecommunications-infrastructure-bill-documents

[7] 5G Cybersecurity Standards — ENISA (europa.eu)

[8] CSI_EMBRACING_ZT_SECURITY_MODEL_UOO115131-21.PDF (defense.gov)

The trusted network would also be suitable for introducing a step-change to avoid disruptive cyber-attacks. It is likely that the nature of attacks seen on the new 6G network will differ greatly from existing techniques due to the differences in infrastructure and protocol usage in the new network. Therefore, understanding and education of this will be important to the evolution.

Having the trusted network should also allow identifying resource usage to be identified by other trusted networks, so that other parties' costs and investments may be shared. This involves at least some level of Service Level Agreement (SLA) between operators to ensure performance for an increasingly diverse set of services (human-related but also machine-to-machine) with different connectivity performance requirements. The GSMA is looking to standardise this approach where third parties can request different network features for the delivery of their data.

The trusted network will provide the following:

- communication
- service provision and creation
- security
- billing
- conformance to legislation
- fraud detection
- ability to communicate to end devices.

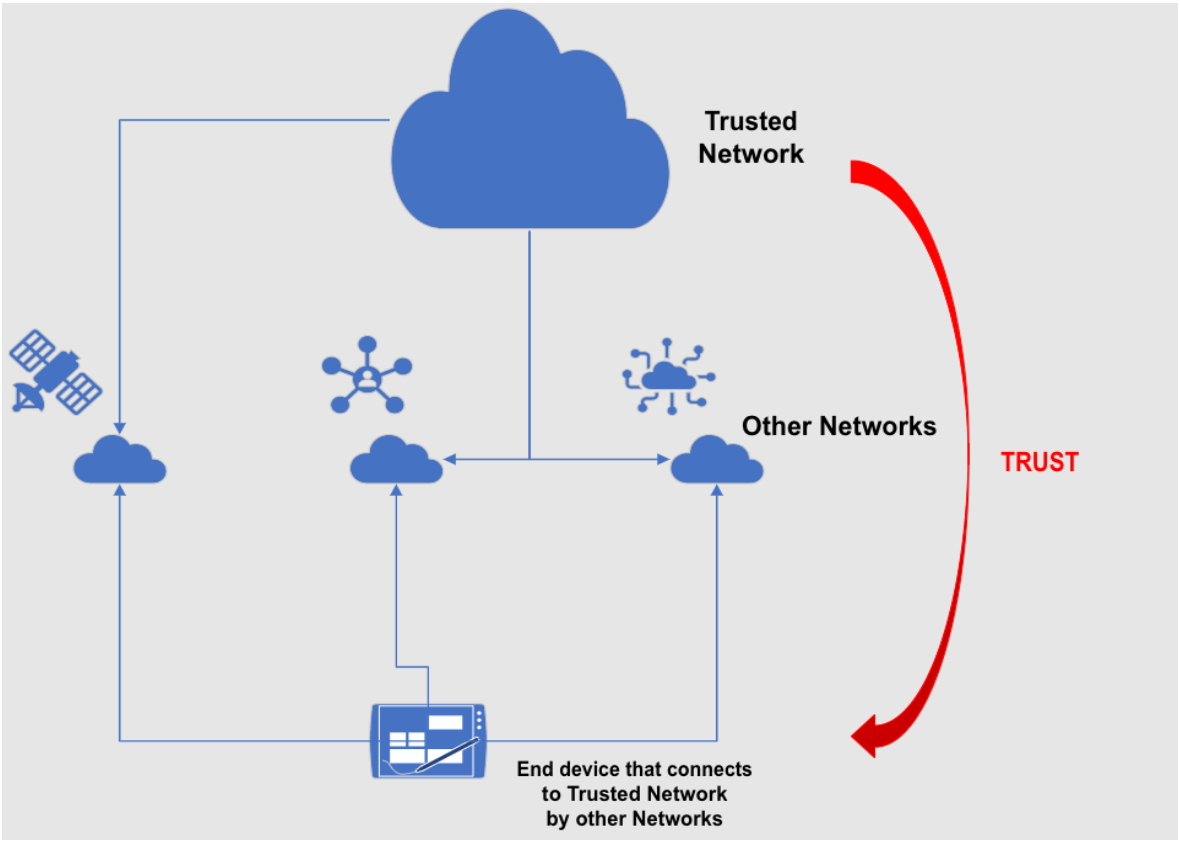

Figure One: A network of networks example

This principle of an overlay trusted network is not novel; in this instance, an initiative was started by the Integrated Adaptive Cyber Defense (IACD)[9] to create such a network. A lot of information currently exists around this topic and should be appropriately consulted when considering this vision further.

Objectives

Risk and Threat Analysis – Trust

The user of any communications system should determine the level of risk they will accept from any misuse or failure of the system, and this risk determination is highly correlated to the level of trust that the user has in the provider and the technology of the communications system.

A simple series of Trust (which should be Zero Trust[10]) concepts should be followed to test and create the security of the whole interconnected communications system. Whilst the term Zero Trust is often applied this may cause problems in interpretation, the aim is not zero trust but rather the starting point is zero trust with an end point of validated trust – knowing why each element is there and trusting that it only does what it is contracted to do. Thus the zero-trust paradigm embraces connection by contract, verification of exactly what operations are being carried out at each node in the connection, and embracing the idea that there is no persistence of trust, rather that trust is re-established every time an entity is used:

1. No other entity should be trusted by default,
2. The Zero Trust architecture should be used to give assurance of the security of the network,
3. No device or user identity should be trusted by default,
4. No protocol should be trusted by default,
5. No third party should be trusted by default,
6. No network or device hardware should be trusted by default,
7. No network or device software should be trusted by default,
8. In the event of trust failure then there should be no method of attacking the whole or part of the system,
9. There should be methods to detect and indicate where trust has failed,
10. Threats from other Networks, Customers/Users, Staff, third parties, Governments, Companies, and Ransom/Hackers should be contained,
11. Denial of Service attacks should be a consideration in the whole design including the Trusted network, connections, services, and protocols,
12. The connection of the Trusted network to the endpoints should be dynamically reconfigurable, to allow communications to continue to take place in cases of disruption,
13. The system must be resilient to classical and quantum cryptanalysis and employ quantum resistant cryptographic algorithms.

[9] https://www.iacdautomate.org/aboutiacd
[10] Zero Trust Maturity Model Version 2.0 (cisa.gov)

Business Requirements

The users (and stakeholders) of a communications system include the Operators, Virtual Operators, Businesses, or simply anyone or anything that wants to connect to, and manage, end devices worldwide. It should also be useable in multiple environments including factory (industrial) and business spaces (commercial, retail, wholesale) and in distributed systems including logistics, as well as in multiple scenarios including those supporting Civil emergency response. The nature of 21st Century business is that connectivity is essential and that that connectivity and the providers of it are dependents of the business users. An untrusted partner in business should not be acceptable to the business and therefore every step should be taken to ensure trust. Again this is where change in business practice has an impact and the nature of a mutable telecommunications network requires the management of the trust relationship to change. What the Zero Trust approach does is, essentially, to take account of mutability and to prevent the carrying forward of trust decisions from time *t* to any future time. An alternative term for Zero Trust is "Verify before use": This applies the Kipling[11] criteria and requires that trust is determined from the answers to each of the following queries --- **What** and **Why** and **When** And **How** and **Where** and **Who**. In simple terms if something is required to connect it should be trusted only if it is known what it is, why it is there, when it is working and how it is working, where it is and who has liability for it.

The level of trust required of a communications system should be easily determined by the user and should be related to the level of perceived and potential threat translated into risk. An end user should be able to choose those networks and network capabilities that offer support of their required risk profile and thus, in collaboration with the provider, ensure trust in the system.

As communications systems are not offered for free, there must be a trusted billing mechanism, together with associated fraud management services for the detection and remedy of errors and frauds. It must allow conformance to regulatory requirements.

Service provision and lifetime requirements - the ability to bring into service, upgrade and cease service should be easy to set up.

Management of the whole Trusted network should be secure, easy and allow third-party control. The problem is that once in the public cloud, it could become difficult to determine where data and policies reside. As part of security ownership, this could allow these to be more easily maintained and owned.

The communications system should allow resource usage by other trusted networks to be identified, so that third party costs may be shared. This will allow appropriate recompense to be built in where other trusted networks are used to provide service.

Present systems, such as Over-The-Top (OTT) providers, do not allow this to happen and a change is required to allow a fair allocation of resources and a realistic way of providing for the use of a service. Spectrum pricing is the only model at present, and this does not seem useful as a model for a network of networks. This is essentially what some service providers use over existing networks.

[11] From Kipling's Just So Stories, published in 1902.

Detail

Intelligent Trusted Network Description

The ITN must be able to support multiple other different lightweight networks, as well as standardised low-trust interfaces to these.

These interfaces will be many and varied and should be configurable to allow for modification and improvement. Example configurations are:

1. Lightweight low-trust Radio interfaces
2. Terrestrial networks
3. High Altitude Platform Stations (HAPS)
4. Satellite networks
5. Earth Stations in Motion (ESIM) (e.g. may be roaming)
6. IP networks in general
7. Mesh networking
8. Other systems (DECT[12], TETRA[13], etc)
9. Can be virtual, on-premises or self-hosted
10. Low-cost IoT devices that a homeowner may purchase and install themselves

These different access modes may be associated with very different size, weight and power constraints which may exert a significant influence on which authentication protocols that are computationally affordable and fit within the available bandwidth.

Many of these other networks may have untrusted parts, so it is important to include a Zero Trust concept to secure the network overall – allowing for safeguarded endpoint communication.

Supporting Security Functions

The ITN is envisaged to have many security, privacy-protection and connectivity functions to support the business functions that use it. Many of the operations may be simplified depending on the business requirements and use, but examples are:

1. Roaming to other trusted networks (sometimes via hubs).
2. Mirroring to back up trusted networks.
3. Authentication/attestation between trusted network functions.
4. Filtering and rule engines between trusted networks (firewalls etc.), including AI/ML monitoring.
5. Customer, device and service provision.
6. Concept and realisation of trust limit between trusted network functions.
7. Dynamic allocation of resources.
8. Introduction of new services (e.g. Group Call) by simple flows or schema.
9. Billing and reconciliation digitally signed and authenticated.
10. Devices of all kinds (mobiles, IoT, Automotive to be flexibly defined as example user cases).

[12] https://www.etsi.org/committee/dect
[13] https://www.etsi.org/technologies/tetra

11. Signaling interaction by traditional telecoms (e.g., SS7, IP) and other protocols which can be defined flexibly.
12. Signaling interaction over http2 (5GSA) and future protocols.
    a. Legacy devices or services on legacy networks sandboxed away.
13. Secure Management by means of a management function. For example, there should be a method for securely managing access to assets and processes, and this must identify both the role and the individual or entity and log the record of activity.
14. Authentication, privacy and quantum-resistant security secret key protocols.
15. Lawful access for location inference and disclosure capability. This is required for the legitimate operation of networks in many jurisdictions, and should be provided in a standardised way where required.
16. Data protection security requirements (e.g. GDPR, storage and privacy, retention limits).
    a. Flexible enough to allow for fraud and security investigations e.g., retrieval by request.
    b. Able to mask personal data where necessary but still allow investigation with escalation if needed.
17. Built in fraud and transaction reconciliation within a trusted network.
18. Integrity, authentication, and data privacy of all protocols.
19. Should be able to be virtual in cloud-trusted networks and RANs.
20. Ability to run and interwork a trusted network just as easily as you can run and interwork an email server today, and the ability to access any network by default, requiring any exchange of funds as necessary.
21. Traditional services are voice, messaging, internet access, entertainment services, and ever-increasing bandwidth.
22. Off-load to Edge Compute and vice versa.
23. Ability to buy higher bandwidths if you want to pay for them (network slicing).
24. Support for the development of the IOT industry which will just continue to grow organically (rather than see the explosion that has been long predicted):
    a. GSMA IoT SAFE[14] – enrolment/provisioning
    b. Other PKI-based provisioning and enrolment (e.g. cloud provider)
    c. DTLS, MQTT, Matter
    d. MUD[15], DPP[16]
25. AI (Artificial Intelligence) to communicate with users, network management, configuration, smart re-configuration, security issue detection and response.
26. Support for trust attestation beyond STIR/SHAKEN[17].
27. Requirement for hardware roots of trust to help industry adoption and reduce the ability to compromise sensitive payloads.
28. Clear delineation between network operations and security-related functions.

[14] https://www.gsma.com/iot/iot-safe/
[15] https://www.nccoe.nist.gov/projects/securing-home-iot-devices-using-mud
[16] https://www.nccoe.nist.gov/sites/default/files/2021-10/09-nist_nccoe_iot_dpp_DNH_slides.pdf
[17] https://en.wikipedia.org/wiki/STIR/SHAKEN

End-User, Device and Customer Perspective

End users (or entities) should be directly and securely handled by the Trusted network which owns them. This should allow secure communication via the Trusted network that owns them, and less trusted networks can therefore safely be ignored as possible security and attack points.

There are many ways a customer uses connectivity. Some examples are:

1. Ability to connect to any access network, based on whatever tariff is appropriate through a central financial clearing process. This is an extension of the way wi-fi is used today based on permissions or funding e.g., through advertising today,

2. Possibly a set of terminal/app developments that cause high levels of uplink data e.g., 'watch my world' services based on worn cameras,

3. Fully immersive services – "live" multi-sensing – e.g., touch, multi-haptic feedback, vision, gestures. Initial implementations are in games but this spreads into the personal communications space too. These require low-latency, high-bandwidth connections and high-capability UE and graphics compute. They may be plugged into screens and wearables (e.g., gloves, vests, physical equipment, and vision devices – glasses, Augmented Reality (AR), etc.),

4. Maybe some greater use of AR with terminals that are more sensible to wear, and more folding devices that can consume significant bandwidth.

This is not intended to be an exhaustive list, as networks and services will continue to be created and evolve.

Minimum Baseline Security Standard (MBSS) and Autonomous Security Assurance

The structural heterogeneity and distribution of the 6G network, coupled with the diverse ecosystem in computing nodes and devices, results in a coarse degree of data access management. This may lead to a malicious actor being able to penetrate the security of the edge device and so compromise this aspect of the system. Untrusted computing nodes joining the network may hack user data at the edge of the network and interrupt the operation. Additionally, because of the performance limitations of edge nodes, these devices cannot resist network attacks, such as man-in-the-middle and denial-of-service, which lead to the breakdown of the edge network and instability[18].

In the case of 6G, building a secure supply chain is vital, vendor compliance is a must and security assurance [GSMA NESAS-2.0, ISO], OWASP vulnerability[19], the integrity of any third-party elements - together with trust and privacy - is also extremely important. Attacks and issues that compromise privacy and security often occur in three main areas of the network: the infrastructure layer security, the network layer security, and the application-level security (which consists of User plane traffic, Control plane traffic and Management plane traffic[20]).

Establishing a reliable level of security policies, procedures, and Minimum Baseline Security Standard (MBSS) for all network functions is extremely important to minimize risks[21]. There is a need for centralized identity governance for resource management and user access – the lack of which may cause network exploitation of applications and systems, leading to unauthorized access of user data, log files and manipulation of AI/ML models. A prominent example is poisoning and backdoor attacks for manipulating the data used for training an AI model, with countermeasures for prevention and detection including use of data from trusted sources, protecting the supply chain and sanitizing data. Another attack type are adversarial attacks that target the model in operation by using specially crafted inputs to mislead the model. Such attacks can be mitigated by expanding the training process (adversarial training), introducing additional modules for detecting unusual ingests and sanitizing input data. Attacks that compromise the confidentiality and privacy of the training data or the model's parameters can be addressed with techniques like differential privacy and homomorphic encryption. Additionally, restricting the number and type of queries to the model and tailoring query outputs can help mitigate these risks[22].

Other attacks jeopardize the confidentiality and privacy of the data used to train the model or the model's parameters. They can be dealt with by approaches such as: differential privacy and homomorphic encryption, introducing restrictions on the number and type of queries to the model and tailoring the output to queries. Therefore, a Unified Framework (UF) is necessary to prevent attacks on the AI/ML model, with a centralized assurance procedure used for evaluation and assessment, before moving it to production. Then, on a regular basis, the model should be evaluated to ensure it provides the desired functionality and is sufficiently robust to changes in input data both natural and (potentially) adversarial.

[18] https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP55-MEC_support_towards_Edge_native.pdf
[19] Vulnerabilities | OWASP Foundation
[20] https://www.etsi.org/images/files/etsiwhitepapers/etsi-wp-46-2nd-ed-mec-security.pdf
[21] https://www.etsi.org/images/files/ETSIWhitePapers/ETSI-WP56_Unlocking-Digital-Transformation-with-Autonomous-Networks.pdf
[22] https://www.enisa.europa.eu/publications/artificial-intelligence-and-cybersecurity-research?v2=1

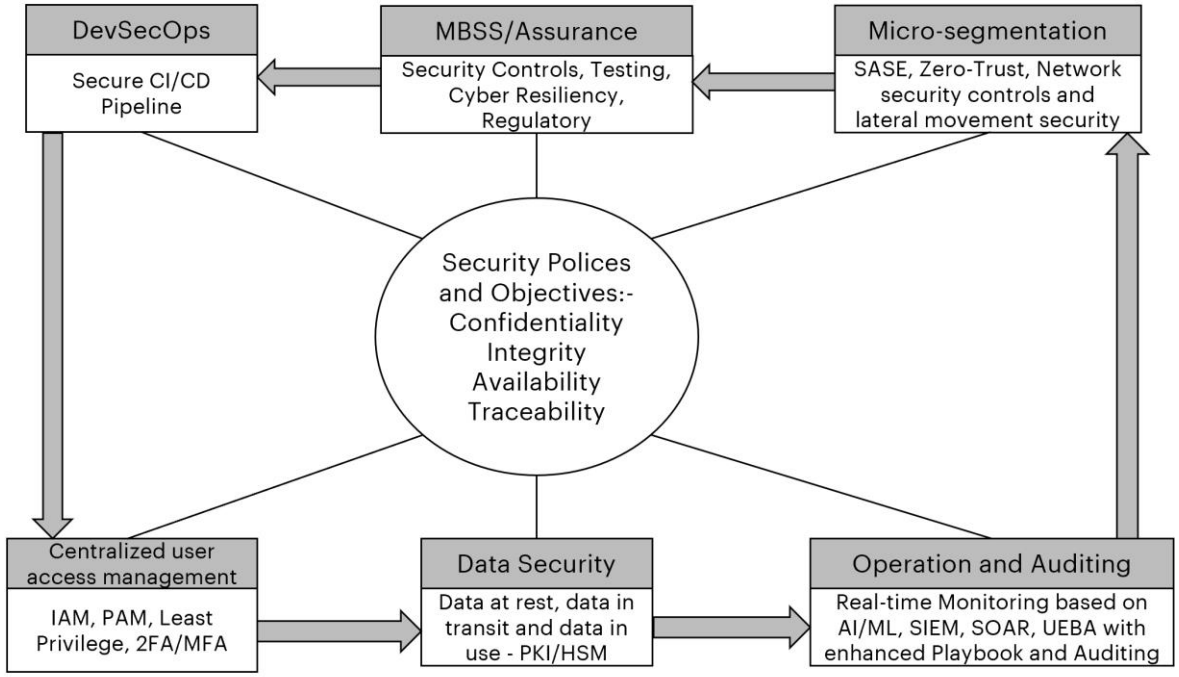

Figure Two: Security Policies and Objectives

In general, 6G and Autonomous Networks require Next Generation Security monitoring with the help of Native Security Agent for Real-Time Security Monitoring and intelligent SIEM (Security Incident and Event Management) with UEBA (User and Entity Behavior Analytics) and SOAR (Security Orchestration, Automation, and Response) capabilities will assistance to enhance the overall Centralized real-time monitoring system of Autonomous Network. See Figure Two[21] for the required security policies and objectives.

An important factor to evaluate is: increasing entry points increases the number of attack surfaces in applications and systems. There are many challenges related to security that need to be considered in future standardization work: Infrastructure layer security, Network layer security and application levels security, Data protection and User security which includes data encryption - at rest, in transit and in motion.

Acknowledgements

Grateful thanks are due to colleagues in TC CYBER, ISG ETI, TC SAI, Industry and Government, BT Group Plc (UK), Azenby Ltd and friends for all the guidance and insight.

Charles Brookson

Laurence Wayne

Scott Cadzow

Faraz Naim

List of Supporting Organisations

BT Group Plc

Zeata Security Ltd

CIS

Maketh Secure Ltd

Cadzow Communications Ltd

Tencastle

Intel

University of Oulu

Sporton International Inc.

Telefonica

Eurosmart

ISAD

Accenture

ETSI
06921 Sophia Antipolis CEDEX, France
Tel +33 4 92 94 42 00
info@etsi.org
www.etsi.org