ETSI TR 103 957 V1.1.1 (2024-09)

Cyber Security (CYBER);
Metaverse Cyber Security Analysis

Reference
DTR/CYBER-00102

Keywords
cloud computing, cyber security, information assurance, metaverse

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

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 Technical Report (TR) has been produced by ETSI Technical Committee Cyber Security (CYBER).

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.

Executive summary

The emergence of augmented reality (also known as metaverse) services in the ICT marketplace has resulted in initiatives globally to consider *inter alia* the potential effects, especially harms, and the need for industry standards. For the most part, the marketplace participants have created their own venues for this purpose, including a particularly significant one in ETSI itself - the Augmented Reality Framework (ARF). Government bodies such as those of European Union also focussed primarily on related strategies.

The security risks envisaged are primarily those of all cloud data centre security combined with a special concern for identity management. ETSI CYBER and ETSI Electronic Signatures and Trust Infrastructures (ESI) Technical Committees have produced related technical publications providing solutions. In general, the security risks and threats are seen as best treated by a Zero Trust Model.

Introduction

Augmented reality is the ability to mix in real-time spatially-registered digital content with the real world. It has given rise to a marketplace for services described as "metaverse" - which is an immersive and constant virtual 3D world built on extended reality platforms - where people and digital objects interact through an avatar to engage in an array of activities. Introduced initially the form of games, the services have been to an array of potential applications.

1 Scope

The present document from the perspective of a use case driven risk analysis, including gaps, applicable to the virtual world (termed Metaverse), respecting environmental constraints, represented as an immersive and constant virtual 3D world where users (people) interact by means of an avatar to carry out a wide range of activities, analyse uniquely new cyber security requirements and technical standards. References to EU/CEPT requirements and ETSI work are provided [i.1] thru [i.5].

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] EPRS PE733.557, European Parliament, Briefing: "Metaverse - Opportunities, risks and policy implications", June 2022.

[i.2] ART Analysis and Research Team, Council of the European Union, General Secretariat: "Metaverse - virtual world, real challenges", 9 March 2022.

[i.3] European Commission: "Virtual worlds (metaverses) - a vision for openness, safety and respect", 05 April 2023.

[i.4] COM(2023) 442/final: Communication from the Commission to the European Parliament the Council, The European Economic and Social Committee and the Committee of the Regions An EU initiative on Web 4.0 and virtual worlds: a head start in the next technological transition.

[i.5] Committees European Parliament: "Virtual worlds - opportunities, risks and policy implications for the single market".

[i.6] ITU-T Focus Group on metaverse (FG-MV), ITU Focus Group Technical Report FGMV-10: "Cyber risks, threats, and harms in the metaverse" (12/2023).

[i.7] ITU-T Focus Group on metaverse (FG-MV), ITU Focus Group Technical Report FGMV-20: "Definition of metaverse".

[i.8] NCSC: "Introduction to identity and access management".

[i.9] ITU-T Focus Group on metaverse (FG-MV), ITU Focus Group Technical Report FGMV-22: "Capabilities and requirements of generative artificial intelligence in metaverse applications and services".

[i.10] Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

[i.11] ETSI TR 103 959: "Cyber Security (CYBER); Critical Security Controls for Effective Cyber Defence; Cloud Sector".

[i.12] ETSI GR ARF 007: "Augmented Reality Framework (ARF); Standards landscape for ETSI AR Functional Reference Model".

[i.13] IEEE SA, IEEE Decentralized Metaverse Initiative: "White Paper - The Industrial Metaverse Report".

[i.14] ITU-T Focus Group, FG-MV-I-494, Focus Group on metaverse, Working Group 3, Draft Technical Specification on: "The Reference Architecture of Industrial metaverse".

[i.15] Metaverse Standards Forum: "Metaverse Standards Register".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

assisted reality: any technology that allows a person to view a screen within their immediate field of vision, hands free

augmented reality: ability to mix in real-time spatially-registered digital content with the real world

digital twin: digital representation of an object of interest

extended reality: umbrella term encapsulating Augmented Reality (AR), Virtual Reality (VR), Mixed Reality (MR), and their underlying technologies

metaverse: immersive and constant virtual 3D world built on extended reality platforms - where people and digital objects interact through an avatar to engage in an array of activities

mixed reality: environment containing both real and virtual components that are seamlessly integrated and interact with each other in a natural way (one end of the augmented reality continuum)

multiverse: multiple metaverses

virtual reality: environment that is fully generated by digital means

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
AR	Augmented Reality
ARF	Augmented Reality Framework

NOTE: ETSI Industry Specification Group.

FG-MV	ITU-T Focus Group on metaverse
MR	Mixed Reality
VR	Virtual Reality
XR	eXtended Reality

4 Survey of metaverse conceptualizations

4.1 Definitions

The ITU-T Metaverse Focus Group dedicated working group on definitions has proposed "metaverse" be defined as "integrative and unified ecosystem of virtual worlds, which is based on interoperable Internet-based and enhanced reality systems and offers immersive experiences to individuals during their digital and synchronous interactions, and new value generation opportunities to organizations." Six explanatory clarifications are included, and proposals by multiple parties seek to change the draft, see [i.7].

The Metaverse Standards Forum provides a Metaverse Standards Register as a publicly accessible database of organizations, specifications, policies, recommendations, guidelines and open-source software related to metaverse interoperability and lists several score bodies, see [i.15].

4.2 Provisioning architecture

Several roughly similar but different provisioning architectures are emerging in different standards bodies. ETSI ISG ARF's augmented reality architecture is depicted in Figure 4.2-1, below, followed by IEEE and ITU-T FG-MV "industrial metaverse" architectures: [i.13], Figure 3 and [i.14].

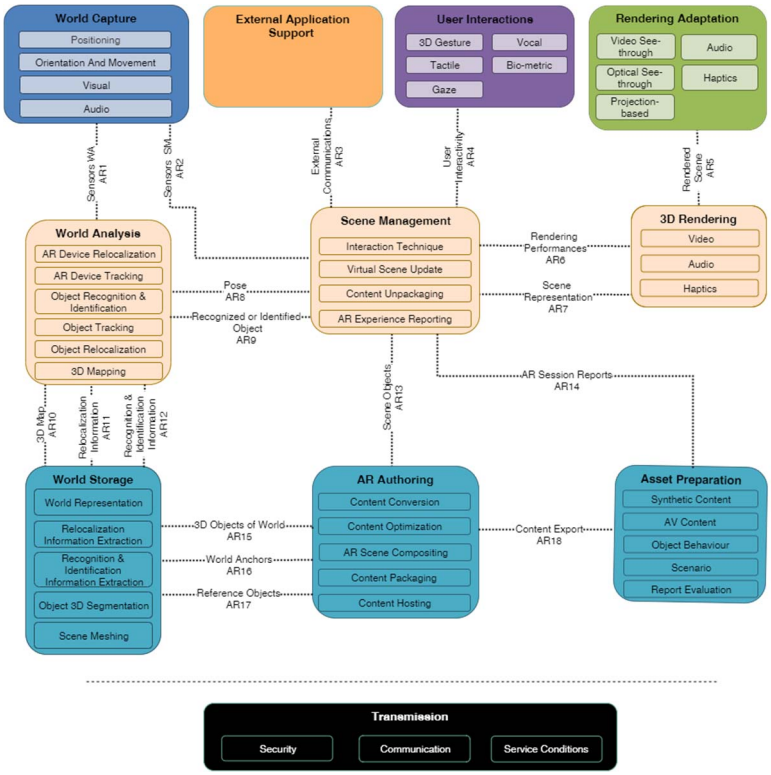

Figure 4.2-1: Diagram of the augmented reality functional reference architecture, (Source: ETSI GR ARF 007 [i.12])

In general, these architectures embrace cloud-based instantiations and network platforms that invoke existing cybersecurity measures.

5 Metaverse use cases, security threats and risk analysis

5.1 Cyber risks, threats, and harms in the metaverse

The ITU-T special metaverse focus group, after an extended period of study, identified the cyber risks, threats, and harms in the metaverse, see [i.6]. Six risks and threats were identified (data breaches, supply chain attacks, fraud, malware, malicious content and poor cyber hygiene), four risks (theft of virtual assets, data theft, data tampering and misinforming), and four potential harms of cybersecurity risks (identity theft and fraud, malware and viruses, data breaches and leaks and social engineering attacks).

It was apparent, however, from the work of the metaverse focus group that identity trust of both users and objects was a special security/safety challenge - invoking what was essentially a Zero Trust Model, see [i.6]. A report on the metaverse identity trust challenges suggests the use of identity platforms recommended by NCSC, see [i.8].

None of the risks, threats, and harms were unique to metaverse service offerings, although some might be exacerbated. Artificial intelligence implementations are also seen as an exacerbating factor, see [i.9]. The group's conclusions were to institute cloud-based controls similar to those published in ETSI TR 103 959 [i.11].

In July 2023, the European Commission as part of its strategy to address Web 4.0 and virtual worlds, called for the development of a toolbox to provide for the use of trustworthy digital identity and digital wallet solutions for safe and secure authentication, virtual transactions, management of digital data and assets, data protection and privacy, consumer protection, cybersecurity, copyright and intellectual property, see [i.4].

The Council of the European Union recently moved forward with proposed regulations on the prevention of the use of the financial system for money laundering or terrorist financing, noting, the development of the metaverse, provide new avenues for the perpetration of crimes and for the laundering of their proceeds, see [i.10].

6 Applicable cybersecurity techniques and gap analysis

6.1 Applicable techniques

In general, metaverse cybersecurity techniques are seen as similar to those already in use. The recommendations largely revolved around augmented reality identity management augmentations and cloud security controls, see [i.6].

6.2 Zero Trust Model for metaverse

Because of the metaverse trust environment is difficult to ascertain and verify, zero trust models are seen essential, see Bibliography.

Annex A: Bibliography

- Metaverse Standards Forum: "Introduction to Metaverse Standards Register Working Group and its projects".
- ITU-T, FB-MV-I-474, IHEID: "Data security and privacy concerns in the metaverse".
- ITU-T, FB-MV-I-409, NCA: "Cyber risks, threats, and harms in the metaverse".
- IEEE: "Towards Zero-trust Security for the Metaverse".
- Spiceworks: "Identity, Access and Zero Trust in the Metaverse Era".
- Medium: "Microservices and Zero Trust: A Match Made in Metaverse Heaven".

History

Document history		
V1.1.1	September 2024	Publication