Metaverse: Security and privacy

October 18, 2022

Heung Youl Youm PhD

Chairman, ITU-T SG17 (Security)

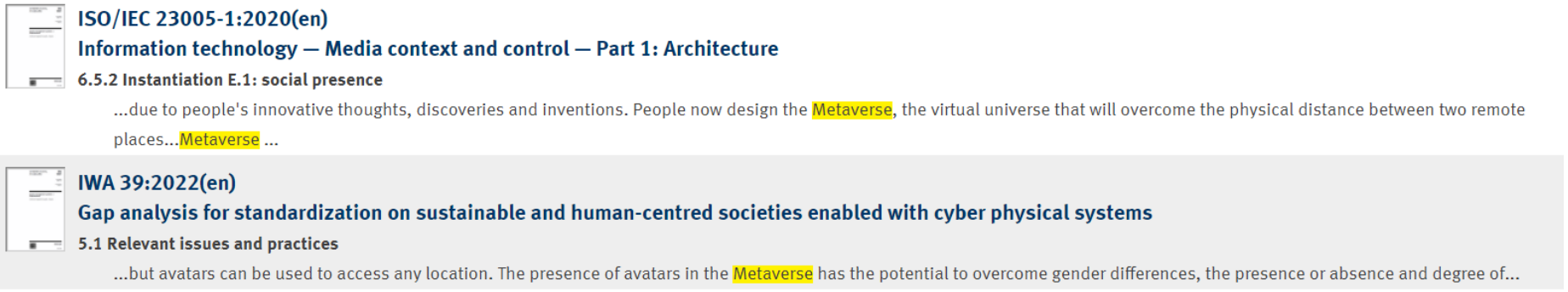
Professor, Soonchunhyang University, Korea (Republic of)

Contents

- Definitions
- Use cases for metaverse in Korea
- Areas for Metaverse use cases
- Key technologies for metaverse
- Asset to be protected
- Example security risks
- Example privacy risks
- Example security and privacy measures
- Concluding remark
- References

Definitions of metaverse

- WIKI
  - a hypothetical iteration of the Internet as a single, universal and immersive virtual world that is facilitated by the use of virtual reality (VR) and augmented reality (AR) headsets
- Other alternative term
  - immersive virtual universe
- No definitions in ITU terms and definitions and ISO OBP
  - Two instances in ISO OBP



ISO/IEC 23005-1:2020(en)

Information technology — Media context and control — Part 1: Architecture

6.5.2 Instantiation E.1: social presence

...due to people's innovative thoughts, discoveries and inventions. People now design the Metaverse, the virtual universe that will overcome the physical distance between two remote places...Metaverse ...

IWA 39:2022(en)

Gap analysis for standardization on sustainable and human-centred societies enabled with cyber physical systems

5.1 Relevant issues and practices

...but avatars can be used to access any location. The presence of avatars in the Metaverse has the potential to overcome gender differences, the presence or absence and degree of...

Example use cases for metaverse service in Korea

- SCH University entrance ceremony in 2021
  - A virtual-reality space in which new freshmen can interact other people with a computer-generated environment, in support of SK Telecom.
  - Soonchunhyang University freshmen attended a virtual welcoming ceremony as avatars through an app.

- ZEPETO
  - Created by the Korea Tourism Organization, a virtual space that mimics Seoul's tourist attractions and induces tourists to visit.
  - Utilizing NAVER’s ZEPETO platform.

Areas for Metaverse use cases

- Immersive entertainment
- Business operations
- Improved education and training
- Enhanced customer experiences
- Work meetings
- Advertising, branding and marketing opportunities
- Digital locations - digital representations of real estate
- Selling digital goods and services
- More connected work experience
- Others to be imagined

Key technologies for metaverse

- Blockchain and Cryptocurrency
- AR/VR Technologies
- 3D Modelling
- Artificial Intelligence
- Internet of Everything (IoE)
- Digital Humans

Asset to be protected

- User profile data
  - Authentication credential data
  - Financial data
  - Behavior data such as user profile
  - Sensitive biometric data
- Data for crypto asset such as cryptocurrency and digital goods and assets, including non-fungible tokens (NFTs)
- Systems for providing services and applications

Example security risks

- Identity theft
- Malware attacks such as ransomware
- Attacks Using social engineering
  - To sell personal data on the Dark Web.
- Risks from using shared spaces
- Bogus information delivery through Deepfake
- Theft for virtual assets such as cryptocurrency and digital goods and assets, including non-fungible tokens (NFTs)

Example privacy and social risks

- Collecting unauthorised data about individuals
- Compromise of privacy principles in ISO/IEC 29100
  - such as:
    - Consent and choice, Purpose legitimacy and specification, Collection limitation, Data minimization,
    - Use, retention and disclosure limitation,
    - Accuracy and quality,
    - Openness, transparency and notice,
    - Individual participation and access,
    - Accountability, Information security, Privacy compliance
- Harassment And Cyberbullying

Example security and privacy measures

- Basic security measures:
  - such as strong password, multi-factor authentication, robust identity management, soft update, anti-malware software, etc.
- Metaverse specific security and privacy measures to be explored, considering:
  - Security measures to prevent security risks
    - Controls in ISO/IEC 27002: such as access control, identity management, supply chain security, cloud computing security, response to security incident, etc.
  - Controls to address privacy risks
    - Privacy controls in ISO/IEC 27701 for data controller and processor
- Especially, defining security assurance is necessary to evaluate the evaluate the degree of confidence of metaverse services.

Concluding remark

- Security by design and privacy by design approaches should be considered from the beginning of the Metaverse services.
- Use risk assessment-based approach to develop new security measures
- Pre-standardization work is critical to provide interoperability for services including security and privacy.
  - FG on Metaverse could be a way forward to address diverse aspects, including security and privacy.
- Security and privacy framework including assurance should be developed.

References

- 10 examples of the metaverse for business and IT leaders, at https://www.techtarget.com/searchcio/feature/Examples-of-the-metaverse-for-business-and-IT-leaders
- TOP TECHNOLOGIES THAT ARE TAKING US TO METAVERSE IN 2022, at https://www.analyticsinsight.net/top-technologies-that-are-taking-us-to-metaverse-in-2022/
- 10 Metaverse Risks To Watch Out Fo, at https://www.theirmindia.org/blog/10-metaverse-risks-to-watch-out-for/

Thanks for your attention!