ITU-T SG17 메타버스 보안 표준화 동향 및 주요 이슈

2025. 9. 16.

나 재 훈

목 차

- ITU-T SG17 구조 및 리더쉽 소개
- ITU-T SG17 메타버스 및 디지털트윈 보안 표준 동향
- 주요 이슈
- Q&A

ITU-T SG17 Structure & leadership

Chair: Arnaud Taddei

Working Party	Questions	Title	Leadership
WP1/17	Q10/17, Q11/17, Q15/17	Digital identity, Quantum based security, PKI and Fundamental security technologies	Chair: Ms Debora COMPARIN Vice-chairs: Ms Honey MAKOLA Ms Afnan ALROMI
WP2/17	Q2/17, Q6/17, Q13/17	Security of IMT, IoT, metaverse and ITS/CAV	Chair: Mr Bret JORDAN Vice-chairs: Mr Yutaka MIYAKE
WP3/17	Q1/17, Q3/17, Q4/17	Cybersecurity and management, security strategy and coordination	Chair: Mr Chang-Oh KIM Vice-chairs: Mr Mahmut ESAT YILDIRIM Ms Xiaoyan BAI
WP4/17	Q7/17, Q8/17, Q14/17	Security of AI, cloud computing services and applications	Chair: Ms Zhiyuan HU Vice-chair: Mr Jae Hoon NAH

목 차

- ITU-T SG17 구조 및 리더쉽 소개
- ITU-T SG17 메타버스 및 디지털 트윈 보안 표준 동향
- 주요 이슈
- Q&A

디지털 트윈 보안 관련 워크아이템

Work item	Question	Subject / Title	Status
X.dtns	Q4/17	Guidelines of using digital twin of network for security	Under study
X.2012 (ex X.smdtsc)	Q7/17	Security measures for digital twin system of smart city	✅ Approved (2024-10-29)
X.2013 (ex X.smdtf)	Q7/17	Security measures for digital twin federation of smart city	✅ Approved (2025-05-29)
X.fr-vsasi	Q7/17	Functional requirements for visualization service in AI security digital twin	Under study

디지털 트윈 보안 관련 워크 아이템

X.dtns, Guidelines of using digital twin of network for security

- Background, Necessity, and Objectives
  - Digital twin networks simulate real networks for testing security
  - Useful for strategy validation, risk deduction, and resilience
  - Guidelines required to ensure interoperability and reliability
- Scope
  - Define functional requirements of visualization services
  - Provide reference architecture for visualization of security assets/incide nts
  - Enhance efficiency and accuracy of network security management

디지털 트윈 보안 관련 워크 아이템

X.2012(X.smdtsc), Security measures for digital twin system of smart cities

- Background, Necessity, and Objectives
  - Smart city digital twins improve operations and resilience
  - Multiple system layers face security threats in data and interfaces
  - Security measures required for reliable urban management
- Scope
  - Identify security threats of smart city digital twin systems
  - Define security requirements across system layers
  - Establish technical and management measures for protection

디지털 트윈 보안 관련 워크 아이템

X.2013(X.smdtf), Security measures for digital twin federation in smart cities and communities

- Background, Necessity, and Objectives
  - Cross-domain digital twins enable collaborative smart city services
  - Security risks include DoS, malicious data sharing, and tampering
  - Federation-wide safeguards are necessary for stable operations

- Scope
  - Describe threats in digital twin federation (e.g., DoS, tampering)
  - Analyze security requirements for federated environments
  - Provide countermeasures and technical safeguards

디지털 트윈 보안 관련 워크 아이템

X.fr-vsasi, Functional requirements for visualization of network security assets and incidents using digital twin

- Background, Necessity, and Objectives
  - Visualization enhances efficiency and accuracy in incident response
  - Current systems suffer from incomplete and inconsistent data
  - Functional architecture needed for digital twin-based visualization
- Scope
  - Define functional requirements of visualization services
  - Provide reference architecture for visualization of security assets/incidents
  - Enhance efficiency and accuracy of network security management

메타버스 보안 관련 워크아이템

Work item	Question	Subject / Title	Status
TR.cr-mv	Q6/17	Technical Report: Cyber risks, threats, and hazards in metaverse	Under study
TR.trust-metaverse	Q6/17	Technical Report: Technical challenges to achieve trust in metaverse	Under study
X.sg-eimv	Q6/17	Security guidelines for enabling integration of identity management across metaverse environments	Under study
X.stm-dpm	Q6/17	Security for things across metaverses in aspect of digital property management	Under study
TR.dpama	Q7/17	Technical Report on "A Landscape analysis for metaverse applications and security"	Under study
X.AA-LLM	Q7/17	Guidelines for Preventing and Mitigating Adverse Attacks in LLM-based metaverse applications (간접 포함)	Under study

메타버스 보안 관련 워크 아이템

TR.cr-mv, Cybersecurity risks, threats, and harms in the metaverse

- Background, Necessity, and Objectives
  - Metaverse expansion introduces new and amplified cybersecurity risks
  - Potential harms include data theft, NFT manipulation, and financial loss
  - Essential to build baseline knowledge for secure metaverse adoption
- Scope
  - Identify cybersecurity risks, threats, and harms in metaverse environments
  - Analyze potential financial, reputational, and operational impacts
  - Provide baseline understanding for further standardization on metaverse security

메타버스 보안 관련 워크 아이템

TR.trust-metaverse, Technical challenges to achieving trustworthy metaverses

- Background, Necessity, and Objectives
  - Metaverse relies on AI, blockchain, AR/VR, and IoT integration
  - Safety, privacy, and identity management are critical challenges
  - Trustworthiness is key for sustainable metaverse development

- Scope
  - Define features of trustworthy metaverses
  - Identify technical challenges in building reliability, safety, and privacy
  - Propose framework for trust-oriented metaverse standardization

메타버스 보안 관련 워크 아이템

X.sg-eimv, Security guidelines for integrating virtual and physical worlds of the metaverse in smart city

- Background, Necessity, and Objectives
  - Integration of metaverse and physical infrastructure offers new value
  - Risks include data tampering, forged control signals, and unauthorized access
  - Guidelines required to safeguard integration enablers in smart cities
- Scope
  - Analyze risk sources of integration enablers in smart cities
  - Define specific security requirements for integration scenarios
  - Provide security measures for safe virtual-physical integration

메타버스 보안 관련 워크 아이템

X.stm-dpm, Security for things across metaverses in relation to data processing and management

- Background, Necessity, and Objectives
  - IoT devices mapped into multiple metaverses create complex data flows
  - Risks arise in lifecycle management, external storage, and access control
  - Framework needed for secure multi-metaverse data management
- Scope
  - Analyze data processing and management issues for IoT in metaverses
  - Define security requirements for data lifecycle, encryption, and access
  - Provide security frameworks for multi-metaverse interoperability

메타버스 보안 관련 워크 아이템

TR.dpama, Data protection of avatars in metaverse applications

- Background, Necessity, and Objectives
  - Avatars hold sensitive personal and behavioral information
  - Privacy breaches may undermine user trust and system adoption
  - Standardization needed to protect avatar data across platforms
- Scope
  - Analyze data types and threats associated with avatars
  - Review current standards and technologies for avatar data protection
  - Recommend standardization activities for secure avatar interactions

메타버스 보안 관련 워크 아이템

X.AA-LLM, Guidelines for preventing adversarial attacks on LLMs in metaverse and digital twin environments

- Background, Necessity, and Objectives
  - LLMs enable natural interaction in metaverse and digital twins
  - Adversarial attacks (prompt hacking, poisoning) pose high risks
  - Guidelines needed to secure LLMs in critical immersive applications
- Scope
  - Identify adversarial attack vectors against LLMs
  - Develop prevention and mitigation strategies
  - Ensure robustness and trustworthiness of LLM applications in immersive systems

목 차

- ITU-T SG17 구조 및 리더쉽 소개
- ITU-T SG17 메타버스 및 디지털트윈 보안 표준 동향
- 주요 이슈
- Q&A

주요 이슈

- AI·메타버스·디지털트윈 보안
  - AI 보안: LLM 공격 대응(X.AA-LLM), AI 기반 서비스 위협 완화, 시각화 서비스 요구사항(X.fr-vsasi)
  - 메타버스 보안: 신뢰 확보(TR.trust-metaverse), 사이버 리스크 분석(TR.cr-mv), 메타버스 내 디지털 자산 관리(X.stm-dpm)
  - 디지털 트윈 보안: 네트워크 DT(X.dtns), 스마트시티 DT 보안(X.2012, X.2013), DT 연합 보안

❖ *중점사항: 차세대 가상환경(AI+Metaverse+Digital Twin)의 위협 모델, 신뢰성, 데이터/자산 보호*

주요 이슈

- 향후 주제
  - Agentic AI 보안
  - Privacy-preserving AI
    - ZKML, FHE, Differential Privacy 기반 AI 보안 급성장
  - Cross-Domain Digital Twin security 확장
    - 스마트시티에 편중
    - 에너지, 헬스케어, 교통, 제조
  - 전자지갑 → CBDC, 토큰화, 자산, 스테이블코인
  - AI기반 자율 보안
    - AI-powered 공격

Q&A