Security Controls and Their Interface

Hexa-X-II Workshop on Enablers for 6G System

Diego López, Antonio Pastor

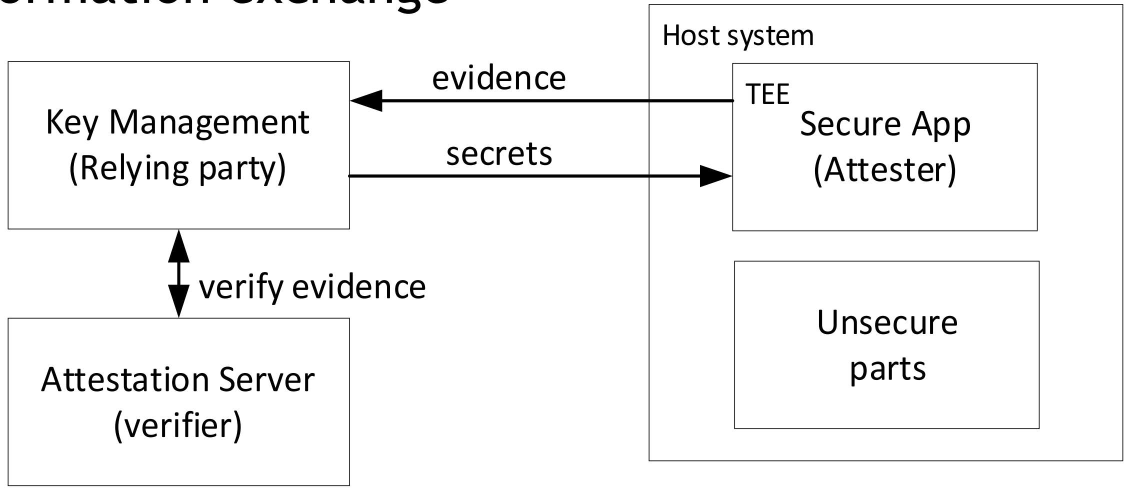
hexa-x-ii.eu

On the Nature of Security/Privacy/Resilience Elements

- Not necessarily intended to provide a new, differential functionality
    - But to address specific threats
    - Providing mechanisms to detect them and to mitigate their impact
    - In our case, associated to the *6G delta*
- Hexa-X-II has identified *threat families* the project intend to address
    - Architectural trends
    - Pervasive use of AI
    - Trust infrastructures
    - Physical layer security
- Mechanisms to detect threats and to mitigate their impact
    - Provided as <u>security controls</u>
    - Components acting as safeguards, detectors, countermeasures…
    - *Enablers for enablers*, if you like
    - Wrapped, when required, by specific enablers
    - Or by orchestration modules, operating *As-a-Service*

Architectural Trends

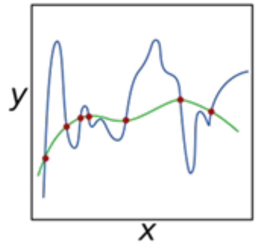
- Key trends with high security impact
  - The NoN (*Network of Networks*) concept
    - Integration of different NSPs, with limited information exchange
  - The Cloud Continuum
    - Isolation, observability, transitivity…
  - Disaggregation, especially in RAN
    - Expansion of the attack surfaces
- Addressing these issues by
  - Formal specifications and formal security proofs
    - Formal descriptions of experiments (for NDT so far)
  - Image attestation
    - Verify how CNFs can be deployed as Confidential Computing applications
    - Analyze, understand and quantify performance impact(s)
  - Topology attestation
    - Protocols and methods for path verification: packet extensions and in-band OAM
    - Performance impact(s) on data and control planes
  - Potential convergence for further consideration



Pervasive (Trustworthy) AI

- AI security implications
  - Attack surface on models and (especially) data
  - Pervasiveness increases impact and complicates detection
  - Go beyond black-box AI, and move towards explainable AI (XAI)
  - AI privacy implications
    - Avoid exposure of sensitive data of any nature, at any stage
- Simulation environment for privacy-enhanced federated learning
  - Privacy attacks to aggregation flows
  - Poisoning attacks to secure aggregation
  - Applicability of partial encryption in local model updates
  - Explore the required balances
    - Privacy and security
    - Security and performance

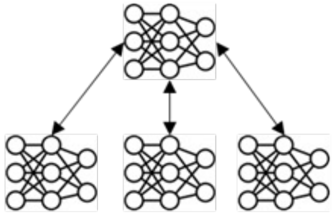
Differential Privacy



Regularization

Homomorphic Encryption

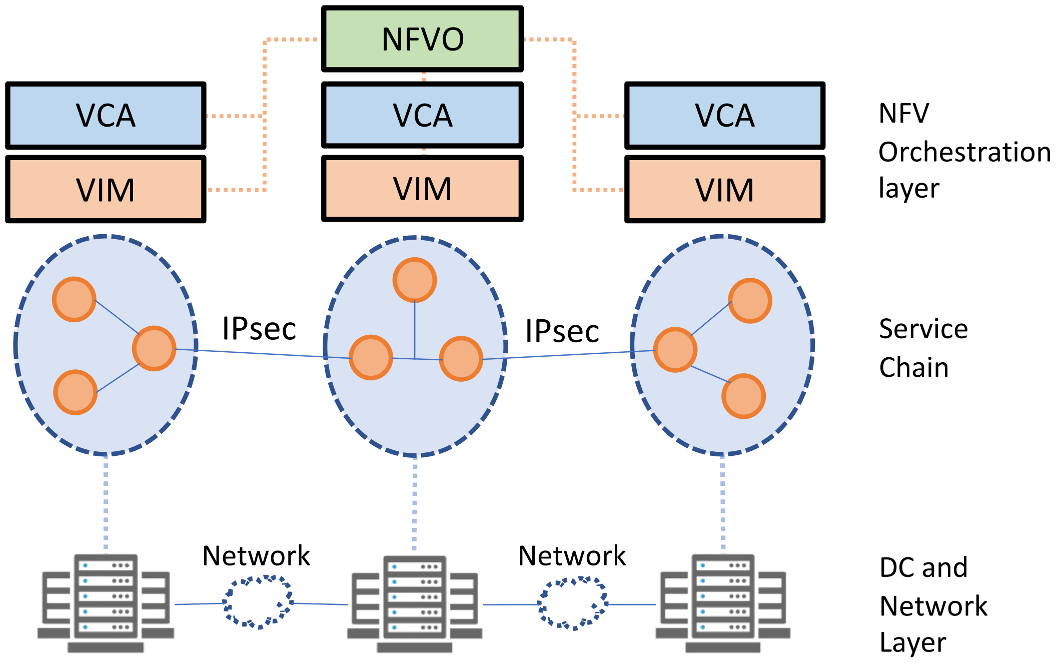
Explainable AI

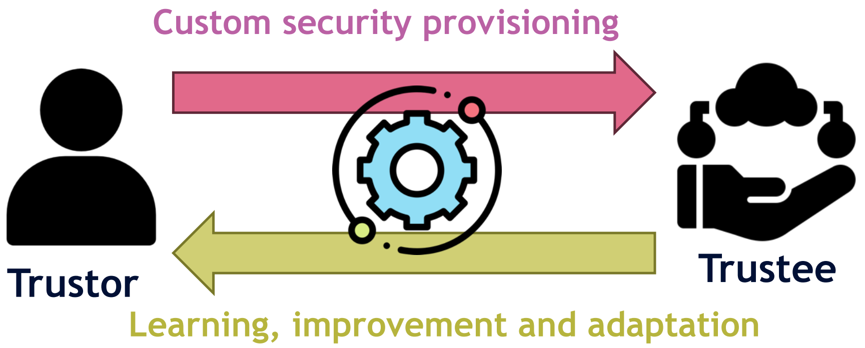


Federated Learning

Trust Infrastructures

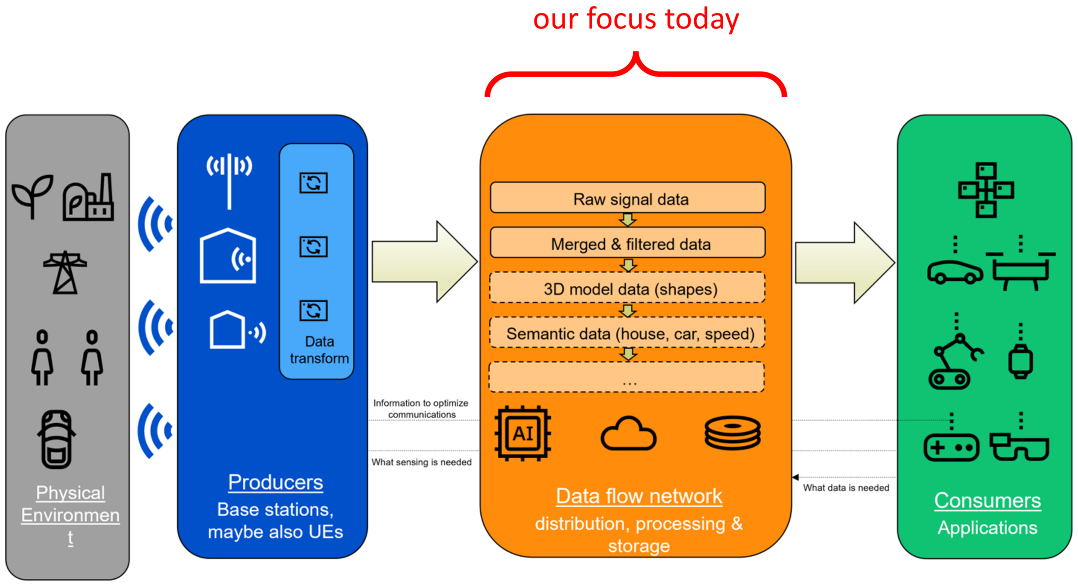
- Consider issues regarding how trust on network services is established
  - Not strictly 6G issues, but to be addressed in the 6G development timeframe
  - Going beyond traditional assurance
    - Making trustworthiness part of service levels, aligned with intent
- Address the transition in cryptography
  - *Agility*, allowing a seamless evolution
  - *Pliability*, adapting to management best practices
- Distributed ledgers
  - As support for *smart contracts*, enforcing agreements
- Experiments in NDT environments
  - With new crypto models
  - PQC and QKD applicability, impact an convergence
  - QKD applicability
  - Management and performance impact on different planes
- Validating the Hexa-X LoTAF approach
  - As a continuation of the work in Hexa-X

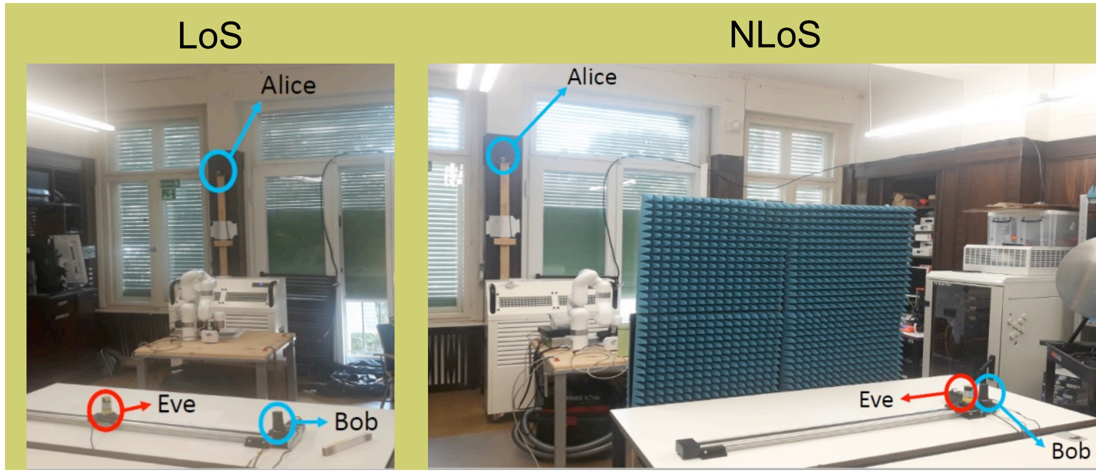



Custom security provisioning
Trustor
Trustee
Learning, improvement and adaptation

Physical Layer Security

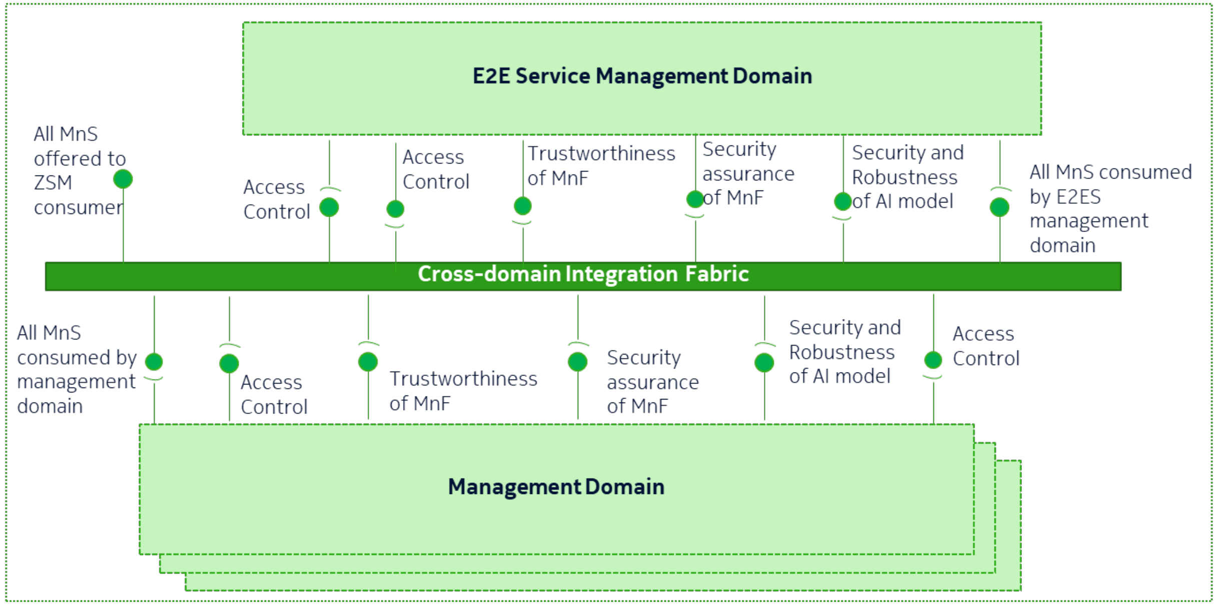
- Extending the threat analysis and mitigation mechanisms to the physical layer
- Context awareness
  - Secret key generation adapted to channel measurements
  - Environment modifications: e.g. blocking LoS, reconfigurable reflectors…
- Security and privacy issues in JCAS
  - CIA (Confidentiality, Integrity, and Availability) of the sensing data flows
  - Applicability and scope of consent mechanisms
  - Threat analysis, applying well-known threat modeling framework for security and privacy
- Sources of physical anomalies
  - Understanding, detection, classification, and localization of jammers, beyond SotA
  - Comparison between expected (DT) and measured RSS at the sensing units
  - Characterization: Jammers, malfunctioning devices, misconfigured neighbor NPNs…
  - Deception techniques to enhance physical security





Security Control Interface - SCI

- A (significant) part of these controls will be used by enablers
  - As a result of design patterns
  - As an evolution of security patterns
- Based on a few basic principles
  - General loosely-coupled model, compatible with the Hexa-X-II integration fabric
  - API-oriented (not necessarily REST in all cases, like crypto)
- Identifying the security controls to be considered
  - Use experiments to characterize these security controls
- And the interface to use them
  - Based on ZSM 014, about to be published by ETSI ISG ZSM
  - Defines a set of security interfaces well aligned with the above principles
  - Validate and extend it as required


E2E Service Management Domain
All MnS offered to ZSM consumer
Access Control
Access Control
Trustworthiness of MnF
Security assurance of MnF
Security and Robustness of AI model
All MnS consumed by E2ES management domain
Cross-domain Integration Fabric
All MnS consumed by management domain
Access Control
Trustworthiness of MnF
Security assurance of MnF
Security and Robustness of AI model
Access Control
Management Domain

HEXA-X-II

HEXA-X-II.EU //

Co-funded by
the European Union

6GSNS

Hexa-X-II project has received funding from the Smart Networks and Services Joint Undertaking (SNS JU) under the European Union’s Horizon Europe research and innovation programme under Grant Agreement No 101095759.