Hexa-X: Trustworthy Networking Beyond 5G

D. R. López, A. Pastor (Telefónica I+D); C.J. Bernardos, A. de la Oliva (UC3M); B. Han, H. Schotten (Uni-KL); C. Morin, C.-T. Phan (BCOM); P. Porambage (U-OULU); P. Schneider (Nokia); E. Ustundag Soykan, E. Tomur (Ericsson)

***Abstract*— Trustworthiness is one of the six main research challenges the HEXA-X project is committed to address to set the foundations of 6G networks. Security forms a basic foundation for all systematization of trust in connectivity, and security considerations must encompass all aspects of cyber-security: resilience against attacks, preservation of privacy, and ethical, safe application of automation to network operations and applications. Security also depends on active management of threat surfaces, including proactive measures such as threat prevention and protection as well as reactive measures such as attack discovery and mitigation. As network services consolidate as essential components in a growing number of application scenarios, their dependability and, equally important, the perception of such dependability as an achievable characteristic, becomes a key feature for network operators, service providers, application developers and, above all, end users. A realistic approach to this trustworthiness challenge must acknowledge that complete security is not achievable, and that all security measures comes with a cost in other terms (such as usability, agility, or swiftness). Therefore, a balance is required in terms of this cost, the risks to be considered, and the impact of a security breach on the mission objectives being served.**

Keywords—6G; trustworthiness; KVI; enablers; architecture

I. Introduction

Trustworthiness is one of the six main research challenges the HEXA-X project (https://hexa-x.eu/) is committed to address, and security forms a basic foundation for all systematization of trust in connectivity. Security considerations must encompass all aspects of cyber-security: resilience against attacks, preservation of privacy, and ethical, safe application of automation to network operations and applications. Security also depends on active management of threat surfaces, including proactive measures such as threat prevention and protection as well as reactive measures such as attack discovery and mitigation. As network services consolidate as essential components in a growing number of application scenarios, their dependability and, equally important, the perception of such dependability as an achievable characteristic, becomes a key feature for network operators, service providers, application developers and, above all, end users.

A realistic approach to this trustworthiness challenge must acknowledge that complete security is not achievable, and that all security measures comes with a cost in other terms (such as usability, agility, or swiftness). Therefore, a balance is required in terms of this cost, the risks to be considered, and the impact of a security breach on the mission objectives being served. The Level of Trust (LoT) of a particular network service in a concrete application scenario is proposed as the essential Key Value Indicator (KVI) to be considered in this regard. The characterization of LoT will constitute one of the main goals of the security task.

Providing the necessary elements for the evaluation of such a LoT is the key goal for a security design and support task, identifying both the applicable technologies to domain experts, and respectively analysing the solutions proposed by these experts in the framework of previous experience and feasible attack patterns. This becomes especially relevant for a project committed to propose next-generation network architectures, so those attacks related to network technology evolution and the increasing sophistication of tools available to malicious actors become especially worthy of attention.

II. Security Aspects

Though it may seem obvious, it is worth recognizing the imperative to apply this security analysis at all levels: for each individual applicable technology, at any plane and layer in the communications stack and any segment in the network architecture) and from a holistic perspective, addressing network services as a whole, including the involved human roles. An initial assessment of these use cases has allowed us to identify a set of security aspects to be considered.

First and foremost, the improvement in the implementation of general requirements such as availability, confidentiality, integrity, and personal data protection.

In what is intended to be an infrastructure heavily relying on dense cloud-based deployments, it will be essential to consider the impact of the use of heterogenous cloud environments and the scaling implications related to massive, pervasive deployments of unattended and untrusted devices.

The nature of the foreseen scenarios for next-generation networks requires real-time data flow protection in new applications such as immersive media or haptic interfaces, the extension of current network security practices to ad-hoc networking, and the consideration of active disruption of network resources to examine the resilience to attacks.

Trust mechanisms should be applied to ensure customer privacy across network segments and providers, and to provision network gear, including authorizations for virtual network functions that may be dynamically deployed on generic hardware.

The generalized use of AI, within the network and by the applications themselves, will require to assess AI-specific threats, including threat surface and attack vectors, the protection of AI data feeds of any nature, from raw monitoring measurements to knowledge sharing, and the direct use of AI by attackers.

III. The 6G Threat Ladnscape

When analysing the 6G threats, and especially those that could be considered as part of the *6G security delta*, the first

category falls within those risks already in today's network practice that can be exacerbated by the advent of faster, more pervasive and dynamic network infrastructures. With the current trend to adopt cloud-native software techniques for designing mobile network functions such as sets of microservices, mobile networks assume an aspect of mainstream IT systems, and are likely to increasingly become a target of the sorts of attacks carried out today against IT systems. A second root cause for security breaches is the failure to stick to sound operational practices in the quest to reach high efficiency in network management. As the complexity of networks rises, the potential of vulnerabilities in the network configuration also rises.

While the overall architecture, features, and deployment models for 6G networks are only starting to take shape, some trends influencing the security posture are already visible, like a huge expansion in the numbers and diversity of end-user devices. Other trends herald highly heterogenous, complex network structures, and potential divestment of responsibility in the variety of stakeholders involved in providing a communication service. All of this increases the potential for vulnerabilities, or in other words, the attack surface.

New technologies likely to be adopted in 6G networks can bring new security risks prominently the use of AI. In the future, attackers very likely will figure out new attacks against new AI methods, taking advantage of the complexity and sometimes unpredictability of the AI mechanisms. Cyber-attackers have a track record of picking up and abusing new technologies quickly, often more quickly than the defenders, and there is no reason for AI being an exception to this trend. As a notable example. AI-based attack methods could optimize the scanning for vulnerabilities, the analysis of huge, illegally acquired amounts of data, or maximize the success rate of spear phishing attacks.

IV. An Overview of security technologies applicable in 6G

In cloud environments, confidential computing provides hardware-based isolation for the processing of payloads, which a cloud provider cannot tamper with. Confidential computing can be used to employ data for AI applications without exposing information by various means, including feeding encrypted data into an enclave, training an AI model without revealing cleartext, and showing only the final model.

Secure digital identities play a fundamental role in building trust. Identities are essential for secure communication in several layers and among several entities in mobile networks. The path to secure identities and protocols depends on establishing trusted identities for infrastructure, connectivity, devices, edge, and network slicing functions.

Attestation is the process of validating the integrity of a system and it implies the integrity of the supporting platform, the software components implementing network functions, and the topology of these network functions to provide the intended service. The attestation steps may be specific to the level of assurance to be established, which, in turn, depends on the required level of trust and the different parties involved in providing and consuming the service.

Privacy enhancing technologies refer to a set of building blocks that can be used to achieve privacy in communications and computations: data anonymization, differential privacy, homomorphic encryption, and secure multi party computations. Depending on the use case, privacy needs, and the threat model they can be adapted alone or in combination. Since each generation of mobile network technologies aim to improve privacy, and with the increasing AI/ML integration in 6G use cases, it is foreseen that these technologies will be embraced to meet the privacy requirements arisen in 6G.

Apart from the wide exploitations in financial applications, DLTs have recently gained a huge attention in the telecommunication industry as well. The key advantages of DLTs are identified as transparency, immutability, non-repudiation, proof of provenance, integrity and pseudonymity which are particularly important to enable different services in networking paradigms. DLT has the potential of protecting the integrity of AI data, enabling the confidence on AI-driven systems in a multi-tenant/multi-domain environment. Smart contracts also open a range of opportunities for network applications that require trusty interactions omitting the need of a third-party authority for integrity verification.

The advent of quantum computers, and their ability of exploring extended solution spaces, is questioning the applicability of computational complexity as it is used by state-of-the-art cryptography. Several solutions are in progress to address this issue. Post-quantum cryptography (PQC), or quantum-resistant cryptography, aims for secure cryptographic systems against both quantum and classical computers. Quantum cryptography follows a complementary approach, with Quantum Key Distribution (QKD) as current practical technology. The main property of QKD systems is that, over public channels, they can leverage the laws of quantum physics to distil keys that cannot be eavesdropped.

While cryptography will remain a key aspect of security in 6G, Physical Layer Security (PLS) approaches can be applied in addition to current mechanisms. These techniques achieve security using unique physical properties of the channel, device or user, and not on computing complexity. Hence, they can be considered quantum-resistant, and do not require parallel key distribution mechanisms. Since PLS does not require to perform complex computations, it can also become a fast and energy-efficient solution, which favours IoT use cases.

Conclusions

The HEXA-X project is committed to seek for a proper definition of the Level of Trust as an essential KVI to be considered for next-generation networks, to analyse how to achieve satisfactory levels considering the threats and enablers discussed above, and to establish the association of this KVI with the perceived, psychological trust stakeholders would be willing to put on the services provided by 6G networks.

Acknowledgements

This work has been partly funded by the European Union's Horizon 2020 research and innovation programme under grant agreement No 101015956 (project HEXA-X).