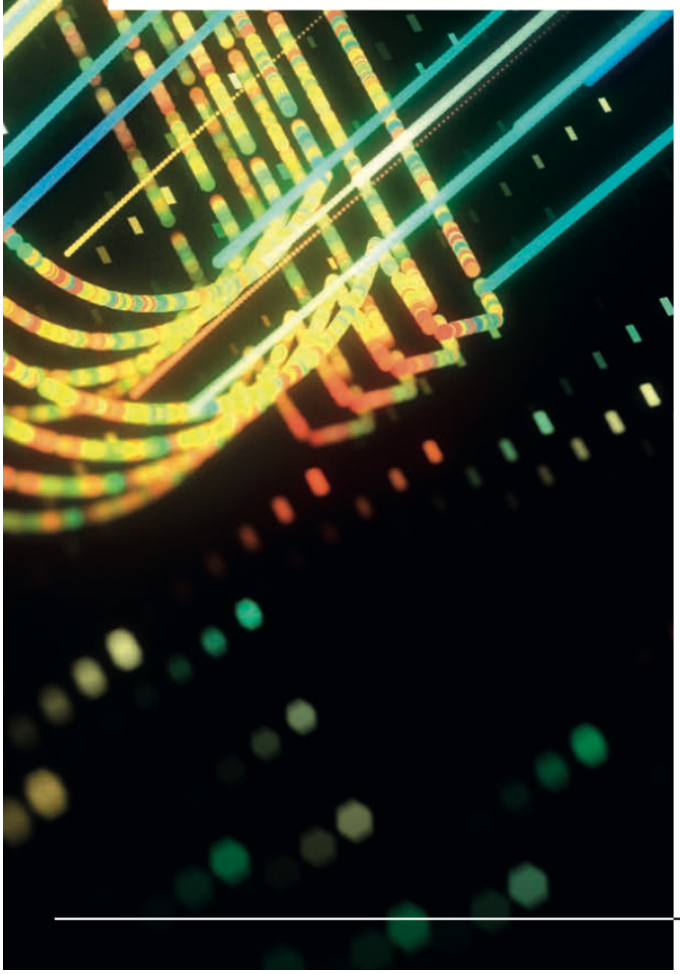
FROM SECURITY-ENHANCED 5G NETWORKS TO SECURITY-BY-DESIGN 6G SYSTEMS

BY DR DAVID SOLDANI, CISO, RAKUTEN SYMPHONY

The fifth generation of mobile communication systems is expanding across the world, adding new possibilities and interest beyond core.



As of June 2021, GSMA Intelligence reported that more than 170 operators have already launched commercial 5G services and more than 60 carriers have announced plans to launch them, having received spectrum across low (≤ 1 GHz), mid (= 1–6 GHz) and high bands (≥ 6GHz), most of them in the Asia Pacific and Europe.

Dell'Oro Group believes Open Radio Access Network (Open RAN) revenues will account for more than 10 per cent of the overall RAN market by 2025. In its Mobile RAN 5-Year Forecast Report, Dell'Oro highlights that the unexpected RAN surge is primarily driven by 5G New Radio (NR). By 2025, 5G NR RAN revenues are forecast to approach $150–200 billion, cumulative 2020–2025 base station shipments will surpass 30 million, and RAN revenues are on track to reach a quarter of a trillion US dollars.

According to the Global Mobile Suppliers Association (GSA), the number of announced 5G devices continues to grow and has now risen to 991, of which 608 are commercially available. By the end of August 2021, GSA had identified more than 470 smartphones, 170 fixed wireless access customer premise equipment devices (indoor and outdoor), 130 modules, 60 modems, 40 hotspots, 20 notebooks and tablets, and 30 other devices (including drones, TVs, vehicle on-board units, etc.).

5G SECURITY CONTROLS AND ASSURANCE

In 5G, the Extensible Authentication Protocol – Authentication and Key Agreement and the 5G Authentication and Key Agreement are used for non-3GPP and 3GPP-authorised access, respectively. Those

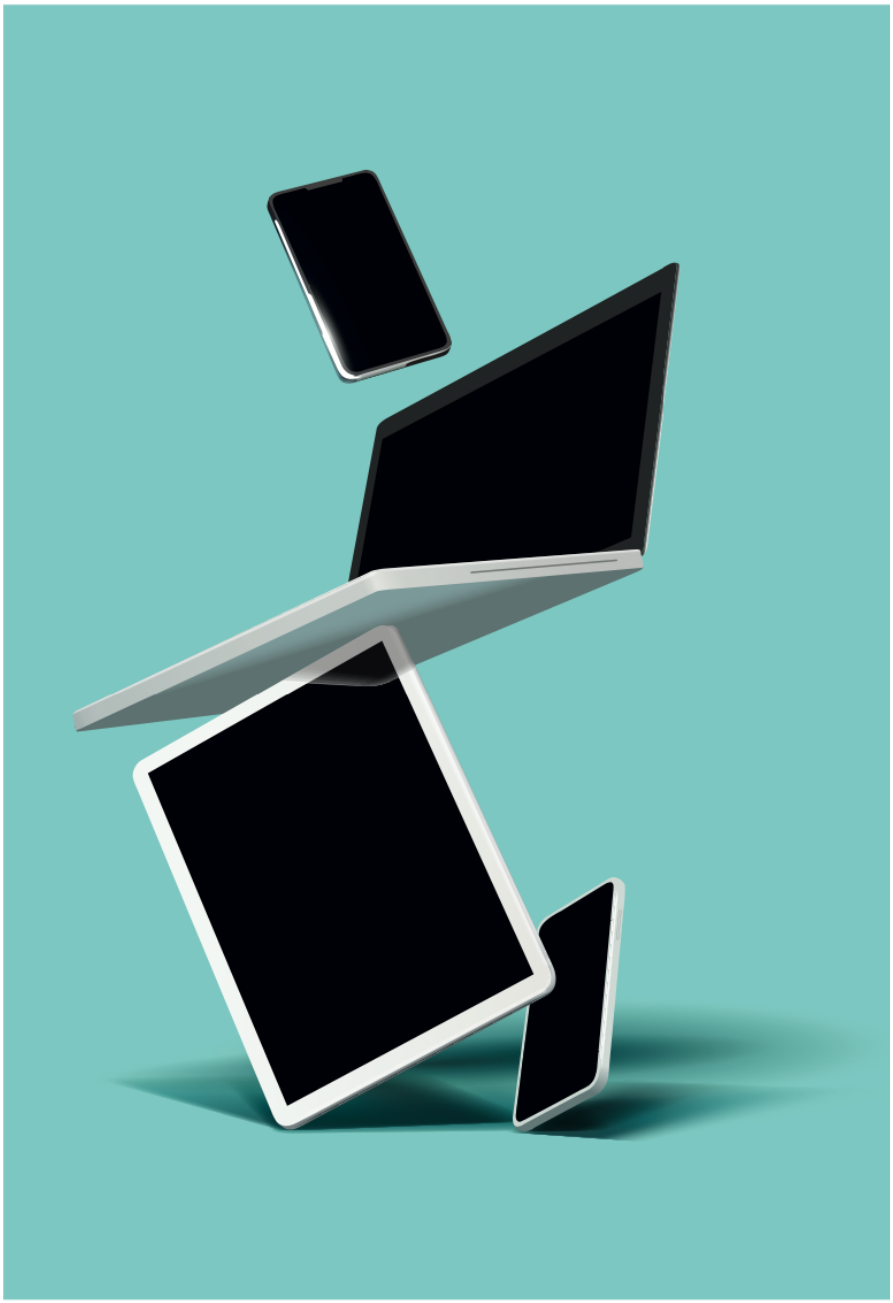
https://www.aisa.org.au/Public/News_and_Media/Cyber-Australia/Cyber-Australia.aspx

procedures allow the mutual authentication between the UE and the network, based on a secret (shared) master key stored in the Universal Subscriber Identity Module and in the 5G core network. The user's privacy is preserved by concealing the globally unique 5G Subscription Permanent Identifier, which can be either in the format of International Mobile Subscriber Identity or presented as a Network Access Identifier.

Moreover, 5G supports security controls for non-public networks; security features for service-based interfaces, transport layer security and token-based authorisation; authentication and key management for applications, such as Internet of Things (IoT) over 5G; and network slice-specific authentication and authorisation.

5G will further evolve the user plane integrity; authentication functions; security controls for rouge base stations, slice enhancement, private networks, multi-access edge computing, and terrestrial and aerial manned and unmanned vehicles; and broadcast channels.

Moreover, 5G supports security assurance requirements and test cases for radio access and core network, data analytics, interworking, and service communication proxy functions, among other functionalities.



SECURITY IN OPEN RAN

The security architecture is further fortified for disaggregated and virtualised RAN (Open RAN). The Open RAN network is cloud native, typically with network functions implemented as containerised microservices.

Open RAN security is built on the following tenets: secured communication between network functions, secure framework for the radio intelligent controller, and secured platform for hosting the network functions.

To support a zero-trust model, O-RAN ALLIANCE has identified several guiding principles for its ongoing work, including supporting integration with an external identity, credential and access management system using industry standard protocols; requiring authentication and authorisation on all access; supporting role-based access control; implementing confidentiality on connections between Open RAN and external components; implementing integrity checking on connections between Open RAN and external components; supporting encryption of data at rest; supporting replay prevention; implementing security log generation and collection to an external security information; and event management.

6G GAINING MOMENTUM

Although 6G is likely to go live around 2030, the number of 6G initiatives underway globally and corresponding investments offer an intriguing prospect for the future. The requirements likely demanded by 6G include as yet unfulfilled 5G use cases and more advanced scenarios emerging for next-generation/6G networks. Examples of

such emerging scenarios include terahertz frequencies, holoportation, tactile/haptic communications, ubiquitous services (land, air, space and sea), imaging and sensing.

In Europe, the European Commission, within the Smart Network and Services framework program, has proposed a €900 million budget to invest in 6G research, with particular attention to standardisation leadership. Beyond that, Japan, Australia, the United States, the United Kingdom, Finland, South Korea and China have each allocated a huge budget to conduct their own research, and there is pressure on other nations to join.

6G wireless aims to bridge the 'physical' and 'cyber' worlds, shifting from connected people and things to connected intelligence. In short, 6G wireless is the technology to realise the fundamental paradigm shift from IoT to the internet of intelligence, the latter being defined as functions with the ability to represent knowledge, process knowledge and make decisions.

PRIVACY PRESERVATION, SECURITY CONTROLS AND ASSURANCE

In general, 6G wireless is projected to be secure by design. To shift from a security-enhanced network to a security-by-design system, 6G needs to integrate security at the heart of the infrastructure and instil the whole network, end to end, with a defence-in-depth strategy. Also, the standardisation process for 6G must provide new mechanisms for security control, security assurance and privacy preservation.

As communication networks evolve, it is expected that there will be increased reliance on artificial intelligence–enabled smart applications requiring situational, context-aware and customised privacy solutions. Hence, the 5G privacy-preserving approach may not be well-suited for future wireless applications due to a diverse and complex set of novel privacy challenges.

One potential solution is the use of pairs of deep neural networks, which can be trained with differential privacy, a formal privacy framework that limits the likelihood that queries of personal identifiable information – sensitive data that can include, for example, the full name of a person, their social security number, driver's licence, financial information, medical records, etc. – could identify a real data subject.

The concepts related to federated learning (FL) are also active topics in the research community for ensuring privacy protection. FL is a distributed machine learning technique that allows model training for large amounts of data generated locally; the required modelling is done by each individual learner in the federation. Instead of sending a raw training dataset, each individual learner transmits their local model to an 'aggregator' to build a global model.

The 5G security architecture, features and protocols simply enhance the mechanisms that constitute the 4G security posture, and 6G is expected to go well beyond that. For example, 6G wireless is expected to support, but not be limited to, the following security controls and assurance mechanisms:

- *Zero-trust architectures:* no asset is trusted implicitly, and continuous access control, authentication and identification are used.
- *Distributed ledger technologies:* immutable, transparent and autonomous ledgers using distributed consensus and cryptography provide an authoritative record of secure transactions.
- *Post-quantum cryptography:* creating quantum-resistant ciphers that future quantum computers cannot crack.
- *Adversarial machine learning:* better evaluate machine learning algorithm's robustness and the development of defences against attacks.
- *Cyber resiliency:* continuous detection and appropriate response to adverse events, and the ability to withstand attacks, and autonomously evolve and adapt to threats.

The GSMA Network Equipment Security Assurance Scheme (NESAS) should include O-RAN security assurance specifications, and industry players, governments, security agencies and regulators are encouraged to adopt the GSMA NESAS for testing and evaluating telecommunications equipment. The NESAS is an authoritative, unified and constantly evolving security assurance scheme for the mobile industry, and could be a part of certification and accreditation processes for current 5G and future 6G network security authorisation in any country. ●

For more information on 6G fundamentals, visit https://jtde.telsoc.org/index.php/jtde/article/view/418

David Soldani received a Master of Science degree in engineering with full marks and a magna cum laude approbatur from the University of Florence, Italy, in 1994. He also holds a Doctor of Science in technology, with distinction, from Helsinki University of Technology, Finland, which he attained in 2006.
In 2014, 2016 and 2018, he was appointed Visiting Professor, Industry Professor and Adjunct Professor at the University of Surrey, the University of Technology Sydney and the University of New South Wales, respectively.
Dr Soldani is currently at Rakuten Symphony serving as Chief Information and Security Officer, e2e, Global. Prior to that, he was Chief Technology and Cyber Security Officer within the Asia-Pacific region at Huawei; Head of 5G Technology, e2e, Global, at Nokia; and Head of Central Research Institute and VP Strategic Research and Innovation in Europe at Huawei European Research Centre.
Dr Soldani can be reached online at www.linkedin.com/in/dr-david-soldani/