Ensuring security and privacy of 5G Networks

ERICSSON

Ericsson continuously works on and supports further increased public and private measures to strengthen the level of security in 5G networks. Such efforts need to reflect the whole space of security enhancements and functional additions including standard, product, network, and operations level. More specifically, Ericsson supports further steps to ensure security on product level, as per the intents behind the EU Cybersecurity act, GSMA/NESAS and 3GPP/SECAM, while we recommend avoiding measures that create a false sense of security such as post development lab testing and source code deposits with third parties.

5G security – going beyond standards

Ericsson welcomes and supports public and private measures to increase the level of security in 5G communications networks and critical infrastructure in general. Much of the discussion around 5G globally is currently focused on security. With 5G, security is not an add-on, but built in from the start as part of the standardization process. That is why 5G is the most secure mobile network generation yet. For more information, please see reference documents at the end of this document.

The 5G standard provides a functional base including the necessary security functionality. However, this is only the beginning to a full answer to a secure 5G network. As 5G becomes a critical infrastructure, what will really determine the security of a network is the security of products, deployments and configurations of networks; as well as operational procedures put on top of the standardized features. Some key security considerations include:

1. **Security capabilities**. Both the hardware and software capabilities on which vendor specific products are developed and manufactured, including the integrity of the vendors' supply chain.

2. **Network deployments**. In addition to the security capability of vendors' products, further important ingredients include configuration security, the application of appropriate hardening according to how the product or solution is used, and awareness of the risks inherent in the specific environment the hardware and software is deployed into.

3. **Operation of networks**. Operational security is significant as both human and organizational failures are present in common causes for security incidents.

When it comes to questions about software embedded in the 5G networks, Ericsson, like most other software providers, conducts software testing during the development phase. Development-time testing has the benefit of providing instant feedback and makes it possible to fix issues promptly as part of normal development before the product reaches the market. This testing is a standard practice followed by most software providers/vendors.

To further strengthen the assurance of security of 5G networks, we suggest taking the following measures:

- Certification schemes in the context of the EU cybersecurity act for critical component to be developed in a joint effort between the industry and the relevant authorities as defined in the Cybersecurity Act (Commission, ENISA, member State representatives, Academia and Industry).
- Security improvements as proposed by GSMA/NESAS for vendor development process accreditation.
- 3GPP SECAM assurance requirements of security functions and product level testing.

NESAS and SECAM will provide information to operators and regulators regarding vendors' security by design procedures and the necessary level of appropriateness of vendors' procedures in the development phase such as:

- Secure Coding Practices
- Vulnerability Management

Security assurance by applying appropriate security testing methods in development phase of software. Avoiding measures that create a false sense of security

Post-development testing is occasionally brought forward as a means to achieve security assurance of live telecom networks. However, we see it as an insufficient tool for the following reasons:

- Lab testing only reflects a limited representation of a network at a given point in time in a specific test configuration.
- Lab testing risk slowing down innovation and delaying time to market, including new security updates, while leading to extra costs in the entire system as modern software development builds on continuous deployments of new releases and functionality.
- 5G networks include many different domains such as radio, transport and core networks as well as end user domains, particularly in the case of critical and massive machine type communication. Critical 5G use cases, such as autonomous driving and manufacturing, will potentially require expanded scope of testing, e.g. including devices and applications for such use cases, further slowing down the development of new industrial business cases. In practical terms, it is difficult in general to draw the line for which products and vendors to include and which not to include, as this may depend on the specific use cases.

Lab testing only reflects a limited representation

- Any post development testing executed, and reviews made on a software and/or hardware product, will always present the security posture of the software and hardware or product at that given point in time, in that specific test configuration.
- A test performed in a lab is a limited representation of the actual network deployment, which is strongly dependent on adaptations, processes and controls. In other words, what is tested and what is running in a live network does not necessarily match.
- A lab test performed on a software and hardware product tests neither for vulnerabilities of the configuration of the live network (point 2) nor for operational security vulnerabilities (point 3) of the live network.
- Certifying software or hardware does not mean it is flawless. Unnoticed imperfections of testing lead to a false sense of security. Generally implementing “Security by design” through evolving industry best practises tend to be the most efficient way to reduce such flaws towards a practical minimum, rather than through “Security by inspection”.

Lab-testing risks slowing down innovation

- Modern telecom systems are developed continuously, and software is updated frequently, for instance to protect against new kinds of attacks and to improve overall system security based on new research. This means that test results of one version of the system do not reflect system behaviour after a software update.
- Every product, release and update for every vendor either covered by the test requirement, or deployed in sectors covered by the test requirement, would have to undergo testing.
- Market acceptance testing centres operate at high pressure from both the reviewed party in a hurry to get to the market and the user side who wants access to the approved end product.
- Vendors begin to limit the frequency and avoid or delay updates due to testing cost and time to market delays. As system security improvements become highly expensive to test, they too are delayed. This slows down the pace of innovation in the sector.
- Weakening security from telecommunication service providers cause delays in the installation of time sensitive, critical software updates due to a lag in market acceptance of lead times in testing centre approval.

Source code disclosure

Recent debate about additional security measures for 5G has included consideration of source code review. This would require vendors of critical infrastructure/public communication networks to deposit their source code with a 3rd party for review hereby vendors losing control over their IPR. This is a worrying development, not only is the measure inappropriate to increase the level of security, but the consequences of requiring transfer and access to source code outside a secure environment of the vendor exposes the source code to uncontrolled leaking. This introduces a new threat to the security of critical infrastructures. We explicitly oppose these measures for the following reasons:

- Source code deposit aka source code escrow is not designed to be a security guarantee for continuously updated system like telecom networks and does not encompass assessment of vulnerabilities.
- IPR loss exposure for companies depositing source code comes with an uncontrollable risk. Next generation networks are built on years of research and development. This intellectual property is protected extensively, hence protecting the resilience of the deployed networks as well. Exporting the IPR from vendor premise increases the risk of losing control over IPR, and thus over accumulated R&D expenses.
- Precedence and domino effect. The introduction of source code deposit and disclosure in one country potentially legitimizes such measures in other countries.
- Definition of critical infrastructure is internationally fragmented leading to an international scope expansion of source code deposits to other strategic technologies, exposing these industries to IPR risks.
- National and international organizations in various trade negotiations have rejected requests to disclose source code to third parties. Proliferation of source code deposit policies inside and outside EU will magnify the negative consequences for a range of key EU industries.

Common Criteria Scheme and alternative approach

Both Common Criteria (CC) and GSMA/3GPP NESAS are intended to help a vendor build better products under the assumption that the vendor is not malicious. The trust model is that the vendor is "trusted but might make mistakes". If the intention is to have a trust model where the vendor is "untrusted and malicious" neither CC nor NESAS will help. In fact, since NESAS provide explicit tests, a customer or authority can check whether the vendor is being truthful. CC does not have that capability, as the evaluation is done by an accredited independent evaluator and not by the customer.

Common Criteria issues:

- The CC evaluation process is too rigid in its requirement for each product to be evaluated, as any patch, update or feature addition will make the certification void.
- From a security perspective, the point above results in yet another problem. Presumably, the patch improves the quality of the product and by restricting the possibility for frequent updates; the overall security of the product is lowered.
- The CC scheme does not have any Protection Profiles ready for the 5G network functions, so the claim that NESAS/SECAM is not yet launched by GSMA and because of that can't be used also applies for CC.
- The development of collaborative Protection Profiles typically takes years to develop and validate. Without collaboration efforts, the specified Protection Profiles risk being inadequate for a wider user community (in EU and globally). In the event there are 'competing' PPs developed the vendors will be put in a very difficult position to cope with country specific protection profiles to certify against. The CC scheme structure in itself does not provide any guarantees they will be able to produce valid protection profiles within any reasonable timeframe. Neither does it provide any chance for the vendors to quickly adapt to massive changes in development processes and methods that CC demands.
- CC's inflexible structure with regards to threats. There is no risk calculation. For a specific product, only one level of assurance is selected. This means that everything deemed a threat is treated equally and requires the same level of tests regardless of the actual risk or impact. For example, we might have one threat that a long-term encryption key is leaked (with large impact) and another threat that one random log post is lost (might have small impact). According to CC these security functions will have the same assurance requirements with regards to documentation, testing and source code verification.
- CC methodology only covers security inspections of a limited and well-defined component, in a specified and confined environment, as defined by the Protection Profile, its usage for system level aspects and supply chain validations is very limited.
- CC is not structured to be able to cope with VNFs, or virtualized products in general, it is structured around 'box' deliveries with HW and SW coming from the same vendor in one product, or at least so that the SW can only be specified to run on a few selected (also certified) execution environments.
- Furthermore, the way the 5G infrastructure is evolving with frequent feature releases and continuous integration and deployments to customer does not work with CC, where one can calculate on 6-month (minimum) certification efforts for every release, for initial certifications one year is probably the minimum with two years certification effort being a typical initial effort.
- CC drives considerable costs for the industry which will result in slowing down the pace of innovation and 5G uptake in Europe – without any other notable benefits than a stamp of approval for a point in time inspection of a product. This does in no way guarantee nor even improve the security posture of any live 5G network.
- This criticism of CC is connected to using it for 3GPP network functions, the IT industry use of CC for routers and firewalls etc. indeed provides value, in the context CC is originally created for.

Possible alternatives to ensure the trustworthiness of a vendor (and its supply chain):

- GSMA NESAS provides means for vendors to have their software development process security audited and accredited by GSMA appointed independent auditing companies. This can provide regulators (as well as operators) with similar level of confidence for the vendor development process security as for instance the ISO 27k provides for companies' Information Security Management Systems.
- The above-mentioned ISO certifications of ISMS (ISO27k), as well as Quality (ISO9k) and Environment (ISO14k), coupled with the scrutiny of all other financial, ethical and legal aspects a publicly traded company adheres to, should give regulators sufficient assurance of the trustworthiness of the vendor.
- The EC should first give ENISA the task to select a suitable certification scheme, and not having individual member states prematurely drive for certifications that has not been agreed on a European level together with the relevant industry stakeholders. GSMA and 3GPP has kept ENISA informed of the progress with the NESAS effort as well as the 3GPP SECAM produced Security Assurance Specifications.
- The NESAS more flexible process by evaluating the vendor regularly instead of each product. Vendor can have their NESAS accreditation removed if not keeping up with the requirements.
- "Security by design" is generally a very efficient tool to reduce vulnerabilities and thereby increase security. Here, best practices and other recommendations are available from e.g. Safecode.org. GSMA NESAS as mentioned above is one such example. The EC could encourage the development and usage of "Security by design" and provide tools and competence development e.g. through its research and innovation program to ensure Europe have sovereign access to tools and competence in this crucial area. This is not limited to 5G networks as such, but also the usage of 5G in various applications and devices like smart vehicles/transport, e-health, smart utilities, hereby benefitting the entire ecosystem required for a secure 5G enabled digital transformation in Europe.

Reference documents
Guide to 5G network security
https://www.ericsson.com/assets/local/news/2018/10201291-04_gir_report_broschure_dec2018_webb_181212.pdf
Ericsson vulnerability management (PSIRT)
https://www.ericsson.com/assets/local/security/psirt-product-security-incident-response-team_rev-a.pdf
Ericsson Security Reliability Model (SRM)
https://www.ericsson.com/assets/local/security/the-ericsson-security-reliability-model_rev-a.pdf

Ericsson.com

Ericsson is one of the leading providers of Information and Communication Technology (ICT) to service providers, with about 40% of the world's mobile traffic carried through our networks. We enable the full value of connectivity by creating game-changing technology and services that are easy to use, adopt and scale, making our customers successful in a fully connected world. For more than 140 years, our ideas, technology and people have changed the world: real turning points that have transformed lives, industries and society as a whole.