Ericsson Review

The communications technology journal since 1924

2014 • 1

Setting the standard: methodology counters security threats

January 29, 2014

Setting the standard: methodology counters security threats

Security has become a central question for network operators and the global telecommunications industry. This is largely due to a shift to more open IP networks, as well as a diminishing dependence on obscure telecom protocols and isolated infrastructure to provide security. The concerns that arise from these developments need to be addressed holistically throughout product development life cycles from creation to termination.

KARL NORRMAN, PATRIK TEPPO, KEIJO MONONEN AND MATS NILSSON

Over the past decade, the number of attacks on IT and communications systems has risen drastically. This increase has gone hand in hand with a massive rise in the use of communications systems for everything from utilities and public health, to transportation and everyday communication. Ericsson refers to this as the Networked Society, and within it, networks serve as critical infrastructure that is fundamental for economic and social development. However, it also leaves society more vulnerable to cyber threats, both malicious and those arising from carelessness and a lack of awareness – it is this situation that needs to be addressed.

As this new threat landscape has become more evident and clearer to both governments and the telecommunications industry, the demand for stronger security requirements on communications equipment has risen, with specific emphasis on telecommunications equipment.

Ideally, the standards that govern the telecommunications industry should provide sufficient security functionality to combat any new threats. However, traditional telecom networks have offered a limited set of functionality, which has in effect provided them with protection. Devices running on isolated infrastructure are by nature less vulnerable than networked ones. Mobile telecom networks have an additional layer of protection provided by the many and very detailed telecom specifications. This situation has now changed dramatically. In parallel with the transition to IP technology, the game changers have been the availability of open source implementations of 3GPP radio protocols and the use of common platforms. As the world moves toward a future in which the impact of these factors becomes even greater, security has become a primary consideration of the telecommunications industry.

To preserve interoperability among products, existing 3GPP telecommunications standards have been developed with a focus on protocols and equipment behavior. The security elements of these standards prevent attackers from misusing systems through the defined protocols and interfaces.

However, the existing standards do not cover how to securely implement protocols and associated functionality in a product, or how to test any given implementation for vulnerabilities. Neither do the standards specify how to secure the proprietary interfaces of a product or how security-related issues should be managed throughout the product life cycle. In other words, security assurance is not part of the 3GPP standards.

As demands for tougher security measures now tend to be discussed on a national level, the risk that different countries will develop diverging collections of security requirements is high. This kind of fragmentation may not only make networks more expensive, but it jeopardizes interoperability and threatens subscriber access to network services and capabilities.

BOX A Terms and abbreviations

CCRA	Common Criteria Recognition Agreement
eNodeB	evolved NodeB
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
MME	Mobility Management Entity
RNC	radio network controller
SCAS	Security Assurance Specification
SECAM	Security Assurance Methodology
SRM	security reliability model
USIM	Universal Subscriber Identity Module

To counteract these potential threats to operator revenue, the best approach to addressing security issues is one that is global and rooted in standardization.

Standardization activities

In mid-2012, Ericsson initiated a 3GPP initiative to stay ahead of the new security challenges. The objective of this initiative was to develop a set of security assurance requirements better suited for a world of ubiquitous connectivity, including a methodology to create the requirements, and a process to ensure that commercial products meet the desired level of security.

For the methodology part, the initial idea was to reuse the ISO/IEC 15408 standard Common Criteria[1]. This approach is often used in conjunction with product certification processes, such as the Common Criteria Recognition Agreement (CCRA), under which product evaluations and protection profiles are performed to high and consistent standards.

However, 3GPP perceived the Common Criteria methodology to be too complex and decided to design a new and lighter one, which would be tailored to meet the needs of the telecom industry – but borrowing from Common Criteria when appropriate.

The new approach goes under the name of Security Assurance Methodology (SECAM), and its study phase has been completed and documented in a 3GPP Technical Report[2]. The formalization of the methodology is documented in the 3GPP Technical Report[3].

The new methodology

The aim of any security assurance methodology – and SECAM is no exception – is to provide users with the assurance that commercial products fulfill the security goals defined by the product's intended use, at a predetermined level of security.

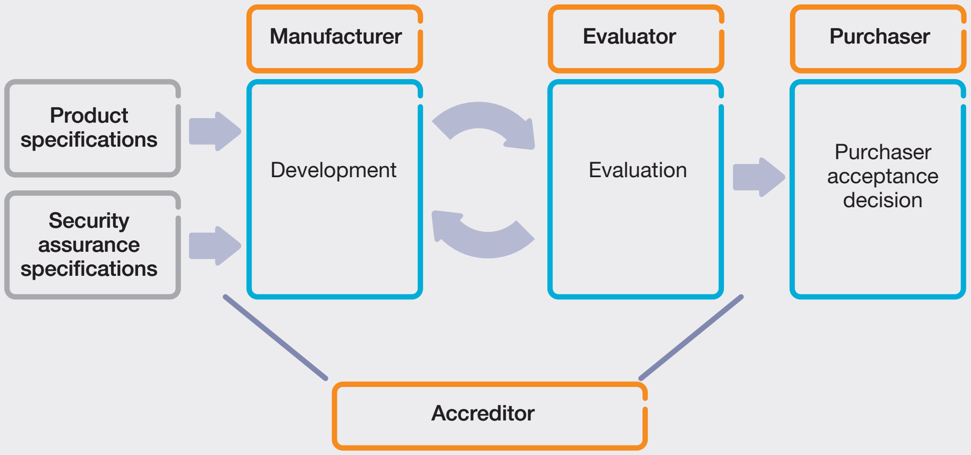
Manufacturers, purchasers and users often refer to products as being secure. The true meaning of such a statement is that a product meets a given set of security requirements, which in the worst case are implicit. But even if a product explicitly fulfills a defined set of security requirements, it may still contain vulnerabilities – it is simply not possible to define every single way a product can be misused. Security requirements can be defined in a negative manner, for example: it shall not be possible for an unauthorized agent to modify the system configuration.

However, there is no way to prove that a product meets such a requirement. There may be ways for an unauthorized agent to modify system configuration that are not known at the time of evaluation.

SECAM differs from previous 3GPP standards in that it establishes security requirements not just for products but also for the development process used to manufacture them.

The methodology applies the following concept of assurance: an accreditor verifies that a manufacturer is capable of producing products to a given set of security requirements, thus eliminating the need to issue certificates on a per product basis. This approach is in contrast to the one adopted by Common Criteria, in which each product is typically evaluated and certified by a third party, and where accreditation requirements relate to the evaluation process and thus fall on the third party and not the manufacturer.

FIGURE 1 SECAM process and roles



Roles, trust relationships and requirements

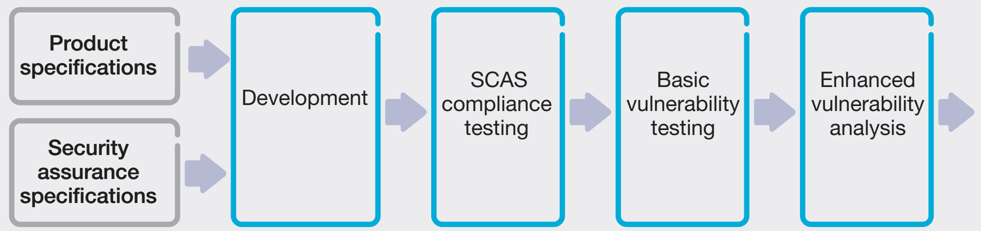
SECAM includes a number of different roles, such as manufacturers and purchasers, and covers a number of trust relationships. Manufacturers build products based on specifications, while purchasers – in almost all cases operators – trust the manufacturer to adhere to the agreed security requirements.

With SECAM, purchasers should be able to trust an accreditor's indirect verification of a manufacturer's development process. As the accreditor only verifies the development process, not the product itself, an additional role is needed to verify that products actually meet given security requirements. This is the role of the evaluator, which could be taken on by a third party. However, it is anticipated – and allowed by SECAM – that manufacturers will assume this role themselves once they have been verified by an accreditor.

These roles and processes are illustrated in **Figure 1**, and once all roles have been verified, purchasers will be able to trust the security of the delivered commercial products.

The accreditor will reassess the manufacturer's product development

FIGURE 2 Product development and evaluation process (according to SECAM)


Product specifications
Security assurance specifications
Development
SCAS compliance testing
Basic vulnerability testing
Enhanced vulnerability analysis

processes at regular intervals to ensure that approved procedures continue to be followed. During these assessments, the accreditor will also verify that manufacturers are able to fulfill the set security assurance requirements, and that the evaluator is capable of performing a proper evaluation of the product.

The specific security requirements that should be set for product development processes have yet to be decided. It has, however, been agreed that these requirements will be set by GSMA – which also acts as an accreditation authority for (U)SIM manufacturers[4].

Self declaration

Once the evaluation of a product is complete, manufacturers can issue a self declaration, which can be used by purchasers for guidance during their buying process. A self declaration includes the results of product evaluations, as well as information about whether the manufacturer and the evaluator are accredited or not.

Using the security requirements and test results defined in the self declaration, purchasers can carry out their own product evaluation. If the results of such a reevaluation are not consistent with the self declaration, the purchaser may initiate a dispute resolution process with the accreditor. Should the accreditor conclude that the accredited manufacturer and evaluator have not acted according to the requirements for the product development process, disciplinary action could be taken, the outcome of which could be the revocation of accreditation licenses.

Security assurance requirements

There are two main types of security assurance requirements in SECAM; these two types are also part of the Common Criteria. The first type relates to the development process and the second to products.

Some examples of requirements relating to the development process include that the manufacturer shall:

- **use appropriate development-site protection;**
- **deploy sufficient version and configuration management;**
- **apply secure coding guidelines; and**
- **ensure that a suitable patch management process is in place.**

Requirements related to products are defined by 3GPP and collected in groups. Several different requirement groups could apply to one and the same product. For example, requirements that are specific to a particular 3GPP function, such as an RNC, a NodeB, or an eNodeB may be collected into one group.

Other requirements, such as those related to platform security and physical protection of the implementation may be put into another group. The purpose of this separation is that same requirement groups may be applicable to several different products and can therefore be reused. For example, a base station that provides eNodeB functionality can apply the requirement group for eNodeBs as well as the group of platform and physical security requirements. A product that provides both RNC and NodeB functionality can apply the specific requirement groups for these 3GPP functions, as well as the same platform and physical security requirements as the eNodeB.

Groups of requirements are brought together under the umbrella of a Security Assurance Specification (SCAS), which roughly corresponds to a Protection Profile in Common Criteria. An SCAS is used as input to the product development process (see Figure 1), and as several requirement groups can apply to a product, more than one SCAS may be appropriate.

Along with the actual security requirements, an SCAS includes tests to ensure that these requirements are correctly implemented. So, a product that passes all of the tests meets the corresponding requirement. It may not always be necessary for a product to pass all tests in an SCAS, though all results should be reported.

It is assumed that management of an SCAS will follow normal 3GPP procedures. In other words, corrections or updates are handled by submitting a change request to 3GPP. Under the current 3GPP meeting schedule, updates can be proposed up to four times a year.

Product development process and evaluation

In theory, the product development and evaluation process consists of four linear steps. In the first step, the product is developed, and then it is tested in steps two to four. Security assurance, however, tends to be executed in an iterative and partially overlapping fashion.

To enable purchasers to reevaluate a product, manufacturers must provide the test results from the evaluation process and the documentation describing the product in the context of the applicable SCASs. If a product fails a test, this should be documented and clearly communicated to the purchaser. An overview of the four steps of the product development and evaluation process is shown in **Figure 2**.

Throughout the initial product development, manufacturers should document how the requirements of each applicable SCAS correlate to specific functions, assets or properties of the product. This documentation is referred to as the SCAS instantiation and is SECAM's closest equivalent to a Security Target in Common Criteria. The primary purpose of the SCAS instantiation is to provide sufficient detail to carry out the required test activities: compliance testing and basic and enhanced vulnerability testing.

Tests should be specified in such a way that a product either passes or fails – partial fulfillment is not an option.

Compliance testing includes, for example, verification that security configuration documentation exists, and that roles for operation and maintenance personnel are properly documented. Tool-driven and manual tests (in which a tester interacts with the product), such as verifying that access to the operations and maintenance function is authenticated, can also be included in the SCAS.

Basic vulnerability testing of a product consists of running a set of security testing tools. Port scanning is one such tool, and this test identifies open ports that should be closed. The testing process could also include the use of tools that exploit known vulnerabilities in both open and closed source software included in the product, as well as fuzz testing of protocol implementations.

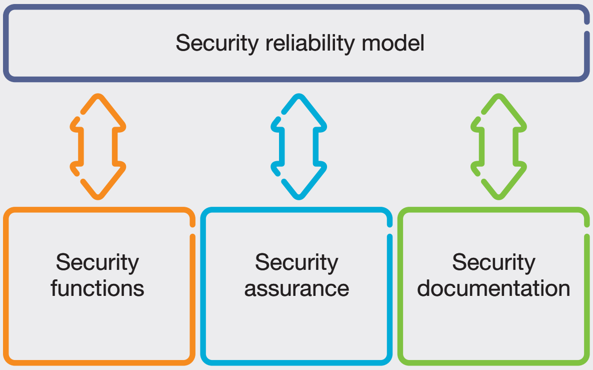
Enhanced vulnerability testing is a more thorough analysis and requires that the tester possesses a deeper understanding of threat analysis and risk assessment than is needed for the previous test steps.

By nature, this type of analysis is hard to standardize, and 3GPP has decided to exclude it from the first stages of SECAM. It may, however, be included at a later stage, when SECAM has reached a greater level of maturity.

Security assurance at Ericsson

To ensure the correct level of security exists in its products, Ericsson has developed a security reliability model (SRM). This model provides a method to set ambition levels for security features and to ensure that an assigned level is achieved in the implementation of a product. SRM consists of three different areas, as shown in Figure 3. The process of setting the security ambition level is based on risk assessment.

FIGURE 3 **Three areas of an SRM**



Within the SRM, security measures are functional requirements defined for products and are divided into different areas. Each area is further subdivided into levels, depending on the risks and threats associated with the product, so that an appropriate security level can be set for it.

In the SRM, a standard set of security assurance activities – such as risk assessment – act to secure design rule compliance, adherence and vulnerability analysis, and configuration and patch management. These activities are a mandatory part of Ericsson's process for product life cycle and are applied to all products in development. Risk assessment is performed early in the development phase of a product, the outcome of which determines what assurance activities need to be applied later in the product-development process.

The configuration and operation of security functions is documented in the customer product information. This documentation is also tested during the functional testing of the security functions. Instructions and guidelines to support users on how to harden the product is also part of the product documentation, as well as a description of the product environment (network, physical and operational) and how it should be designed and implemented. All of this forms key parts of the documentation required by SCASs in 3GPP SECAM.

For Ericsson, the SRM is vital in our R&D processes and provides us with a documented approach to assure that we develop secure products. All of which is in line with the self declaration that is included in the SECAM process.

Way forward

The first step in 2014 in terms of SECAM development will be for 3GPP to develop an SCAS for an MME[5] and formally record the SECAM process in a permanent 3GPP document[3]. In parallel with this activity, GSMA will begin to define the requirements for the product development process, as well as establish the accreditation authority.

Once these two activities have been completed, vendors and GSMA will run a pilot test case of SECAM evaluations.

Ericsson engineers will continue to use their experience of working with the SRM to provide input to SECAM, and conversely, the SRM will be aligned with SECAM. And perhaps most importantly, Ericsson will continue to develop its SRM as a core feature to combat the constantly evolving threats to the communications industry.

Conclusions

SECAM provides a framework to set security requirements that are applicable on a global scale. It also encompasses security requirements and models for evaluating the quality of product development processes, as well as indirectly evaluating the quality of commercial products. In addition, the framework includes tests

»

to ensure that products fulfill the set requirements.

The SRM model puts Ericsson in a good position to fulfill the requirements and help keep future networks secure as they take an ever more central role in society.

Karl Norrman

joined Ericsson Research in 2001 to work in the area of security. His main focus is security protocols and architectures, software security and security assurance. He is currently Ericsson's standardization coordinator for security in 3GPP (SA3 working group) and is the main delegate for the work on SECAM. He holds an M.Sc. in computer science from Stockholm University.

Patrik Teppo

joined Ericsson in 1995 and is currently working as a security consultant and systems manager in the Network Security Competence Center at Ericsson Finland. He is the driver of Ericsson's security reliability model (SRM) and provides back office support for 3GPP SECAM standardization. He holds a B.Sc. in software engineering from Blekinge Institute of Technology, Sweden.

Keijo Mononen

is the Head of the Ericsson Network Security Competence Center. His Competence Center is responsible for driving and supporting network security activities across all of Ericsson's Business Units. Mononen has been with Ericsson for 23 years in various positions both in R&D, the business line and service delivery. For the past 10 years he has worked with security in both R&D and services. He holds an M.Sc. in computer science and engineering from Chalmers University of Technology, Gothenburg, Sweden.

Mats Nilsson

is the director for Product Security within the CTO office. He coordinates the technology- and product-related security activities within Ericsson, including regulatory aspects. In this role, he initiated the 3GPP activities on security assurance and the SECAM standardization. Nilsson is a well-known industry veteran, having held a series of front-line positions within Ericsson since the 1990s, as well as serving as CEO for the Open Mobile Terminal Platform initiative.

References

1. ISO/IEC 15408-1, 2009, Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model, available at: http://www.iso.org/iso/home/store/catalogue_ics/catalogue_detail_ics.htm?csnumber=50341
2. 3GPP, Technical Report 33.805 V12.0.0, Study on security assurance methodology for 3GPP network products, available at: http://www.3gpp.org/DynaReport/33805.htm
3. 3GPP, Technical Report 33.916, Security Assurance scheme for 3GPP Network Products for 3GPP network product classes, available at: http://www.3gpp.org/DynaReport/33916.htm
4. GSMA, Security Accreditation Scheme, Increasing U(SIM) security, lowering business risks, available at: http://www.gsma.com/technicalprojects/fraud-security/security-accreditation-scheme
5. 3GPP, Technical Report 33.116, Security Assurance Specification for 3GPP network product classes, available at: http://www.3gpp.org/DynaReport/33116.htm

Ericsson Review

To bring you the best of Ericsson's research world, our employees have been writing articles for Ericsson Review – our communications technology journal – since 1924. Today, Ericsson Review articles have a two-to-five year perspective and our objective is to provide you with up-to-date insights on how things are shaping up for the Networked Society.

Address:
Ericsson
SE-164 83 Stockholm, Sweden
Phone: +46 8 719 00 00

Publishing:
Ericsson Review articles and additional material are published on www.ericsson.com/review. Use the RSS feed to stay informed of the latest updates.

Ericsson Technology Insights
All Ericsson Review articles are available on the Ericsson Technology Insights app available for Android and iOS devices. The link for your device is on the Ericsson Review website:www ericsson.com/review. If you are viewing this digitally, you can:
download from Google Play or
download from the App Store

Publisher: Ulf Ewaldsson

Editorial board:
Håkan Andersson, Hans Antvik, Ulrika Bergström, Joakim Cerwall, Deirdre P. Doyle, Dan Fahrman, Anita Frisell, Jonas Högberg, Ulf Jönsson, Magnus Karlsson, Cenk Kirbas, Sara Kullman, Kristin Lindqvist, Börje Lundwall, Hans Mickelsson, Ulf Olsson, Patrik Regårdh, Patrik Roséen and Gunnar Thrysin

Editor:
Deirdre P. Doyle
deirdre.doyle@jgcommunication se

Chief subeditor:
Birgitte van den Muyzenberg

Contributors:
Paul Eade, Nathan Hegedus and Ian Nicholson,

Art director and layout:
Jessica Wiklund and Carola Pilarz

Illustrations:
Claes-Göran Andersson

ISSN: 0014-0171

Volume: 91, 2014

Ericsson
SE-164 83 Stockholm, Sweden
Phone: + 46 10 719 0000

ISSN 0014-0171
284 23-3221 | Uen