Ericsson White Paper
GFTL-22:000488 Uen
April 2022

ERICSSON

Evolving Operational Security Assurance for 5G and Beyond

End-to-End Full Stack Security Compliance in Network Function Virtualization

Executive summary

5G networks and beyond are expected to evolve in dynamic and programmable virtualized environments to fulfill the different needs of the emerging use cases of mobile networks. Furthermore, this evolution is set against the background of a new security threat landscape. Thus, these are calling for an evolved approach for security along with security assurance mechanisms providing the confidence that the intended security policies are effectively enforced. To achieve this, an automated end-to-end full stack security compliance approach in network function virtualization can provide the service provider confidence that security and compliance are ensured.

This white paper investigates the main challenges related to the security compliance in network function virtualization for 5G and beyond. It recommends a full stack end-to-end automated security compliance approach in network function virtualization based on five key features supporting the evolution of operational security assurance in addition to the product security assurance.

Content

Introduction

Today mobile networks represent a key part of our daily lives allowing us to benefit from various essential services across various domains (for example, automotive, utility, and healthcare). Thus, they make up an important part of our critical infrastructure, and subsequently, they are becoming an attractive target for threat actors. Therefore, mobile networks need to be securely protected and operated.

To realize these new services and enable economies of scale, 5G leverages several technologies, particularly Network Functions Virtualization (NFV) and Software-Defined Networking (SDN). Thus, 5G (and even 6G) network services are deployed as applications running in NFV-based environments with SDN supporting traffic steering throughout the different components of the service. As NFV and SDN become codependent, the term NFV environment is used to refer to an NFV infrastructure with SDN support.

This new technological shift has increased the complexity of the environment, which now consists of several layers (mainly due to virtualization and containerization), managed using different management components, and distributed geographically across several administrative domains (for example, 5G RAN deployed in edge data centers while 5G core deployed at regional and national datacenters). The aforementioned technologies and the new operational ways have resulted in a new threat landscape (e.g., the dynamic environment leading to more misconfigurations and security compliance drifts) [1]. This change is also accelerated by other factors such as software/hardware disaggregation, multivendor deployments, and shared responsibility in cloud. Therefore, there is a need for security to be addressed end-to-end in a cohesive way on all layers, across administrative domains.

Evolving security assurance for mobile networks

As security is key in the operation of mobile network, a lot of efforts have been deployed by different stakeholders including Ericsson to address security threats, improve the trustworthiness of such a platform and collaborate in developing security assurance frameworks and processes.

Security assurance [2] is defined by the National Institute of Standards and Technology (NIST) as the measure of confidence that the security functionality is implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system—thus possessing the capability to accurately

mediate and enforce established security policies. In the context of mobile networks, the Network Equipment Security Assurance Scheme (NESAS) [3] has been jointly defined by 3GPP and the Global System for Mobile Communications Association (GSMA). The latter provides a security assurance framework that defines a set of security requirements and an assessment framework for secure product development and product lifecycle processes using 3GPP security test cases defined in Security Assurance Specifications (SCAS) documents. With the virtualization of those products, SCAS and NESAS were adapted to evolve security assurance to assess virtualized mobile network applications. This framework is meant to benefit the vendor and operator and increase the trust in the vendor as well as in the security of its products. In this context, Ericsson products such as cloud RAN [4], 5G Core and transport technology [5] have successfully passed the independent NESAS security audit.

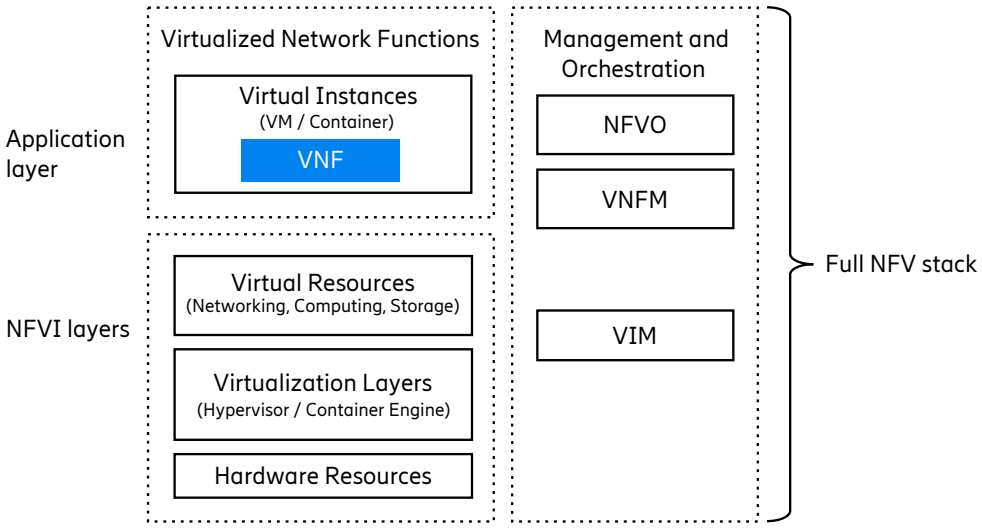

Figure 1. Full NFV stack consisting of several layers for realizing virtual network functions

However, NESAS scheme focuses more on the application layer implementing the functionalities of the mobile network products rather than on the environment hosting them. To fill this gap, operational security assurance as defined by ETSI in [6] (and adopted by [10]) can be leveraged to provide the ground for confidence that the security controls are running as expected in operational system in a multi-layer virtualized environment such as NFV. Figure 1 shows a high-level overview of the full NFV stack consisting of multiple layers. In such a multi-layer environment, some attack vectors can target one layer left without sufficient protection and assurance, giving an attacker a foothold within the environment, and opening the door for him to move laterally to compromise other layers. Thus, security protection and assurance should encompass all layers.

Furthermore, not every security issue can be addressed at only one level in these complex

systems; the security issues often need to be tackled by a coordinated coherent solution encompassing different layers. For example, a secure virtual mobile network product running on an unsecure environment can be exposed to security risk of an intruder exploiting vulnerabilities in the environment or maliciously changing the configuration to some unsecure values. Using consistent and comprehensive security policies can mitigate such risks. These policies should be managed by the service provider rather than by the vendors of the mobile products and are generally dependent on the service provider's tolerated security risks, the security context, and the relevant regulations and standards as well as the ability of the service provider to accurately translate those requirements to appropriate policies. Additionally, as several layers and administrative domains generally manage their own security policies, there is a need to enable full stack and end-to-end consistent security policies. Security controls and processes based on incomplete and inconsistent security policies create risks of unnoticed security holes that can be exploited by attackers. In summary, although vendors need to subject their products to security assurance, the delivered products need to be securely configured and managed by the service provider in addition to be operated in an assured secure environment.

This naturally calls for an end-to-end approach to security assurance that includes the full stack, supports coordination across layers, and utilizes automation for speed, decrease of manual effort, and mitigation of human error. Thus, new mechanisms are required for automated and coordinated security compliance monitoring, verification, orchestration, and enforcement in an NFV environment.

This white paper recommends an end-to-end full stack automated security compliance in NFV to support operational security assurance for 5G and beyond. Figure 2 shows a high-level overview of the recommended solution. In the following, we first discuss the main encountered challenges towards this recommendation and then describe five key features that we envision to realize operational security assurance.

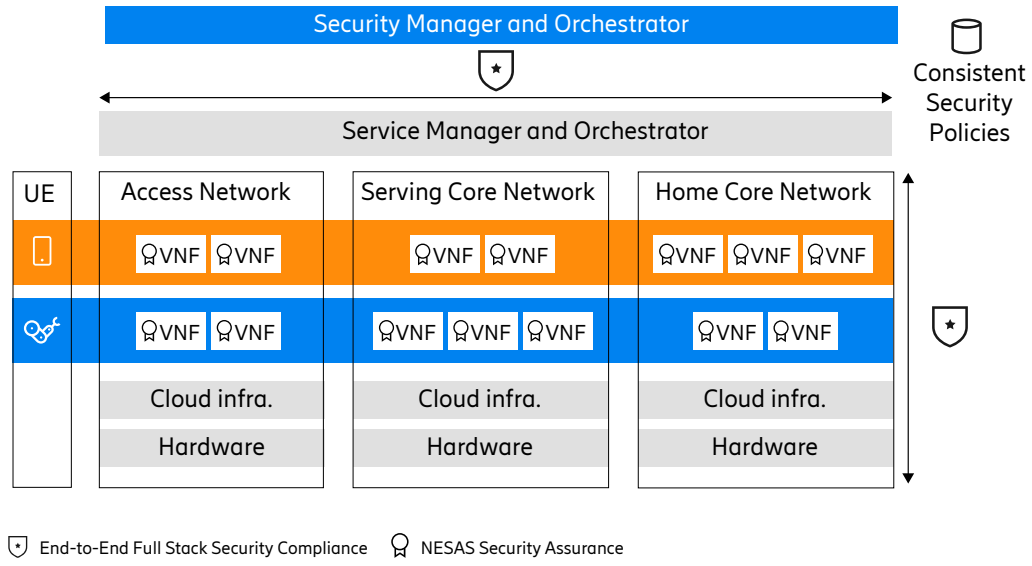

Figure 2. Automated end-to-end full stack security compliance in NFV for operational security assurance in 5G and beyond

Challenges of end-to-end full stack security compliance

Protecting next generation mobile networks requires taking into consideration protection of the full stack and addressing the evolving security threats. Therefore, the right security controls must be deployed in the right place and must be configured consistently with the security policies to correctly address those security issues. Additionally, appropriate mechanisms must be in place to ensure that those controls stay adequately configured during operations. Furthermore, with the advent of new security threats, policies need to be updated and appropriately enforced through the deployed security controls to address those new issues. To achieve this, continuous and automated security compliance verification, and enforcement approaches, encompassing the full stack and end-to end, can help providing such assurance. However, achieving this requires overcoming several challenges.

In the following, the main foreseen challenges for automated monitoring, verification, orchestration, and enforcement of security policies in NFV environments are summarized.

Challenge 1: Highly dynamic and complex environments

With the increase in the adoption of 5G by different consumers and various verticals, the size and complexity of the underlying NFV environment is expected to grow rapidly. To respond to such a surge in demands and satisfy new requirements while decreasing cost, operators have been adopting new strategies to deploy mobile networks over cloud environments involving different management domains and adapting multi-vendor solutions. These introduce challenges related to shared compliance responsibility and how to coordinate and aggregate security compliance management across layers. From another angle, the dynamic orchestration and scaling of deployed services will consequently call for even more automation support in service deployment and orchestration as well as in the security management of these services. To further increase the dynamicity, the pace of the product release life cycle is expected to increase, and thus, modifications to the services and environment will be frequent. Finally, the additional complexity is added as the mobility of the services in different domains (for example, from the core to the edge) requires aligning at run time compliance with requirements and risks in different domains (for example, different providers and data centers).

Challenge 2: Changing security landscape and security policies

As the security landscape can change rapidly (for example, by the discovery of new vulnerabilities) and changes to the environment can occur frequently (for example, migration of VNFs between domains or updates to VNFs and their configurations), policies might also need to be updated to suit new requirements and the new security context. Consequently, the security controls need to be updated and then monitored and verified against the new policies to stay aligned with requirements and tolerated risks. However, currently, there is a lack of well-defined operations and maintenance interfaces and application programming interfaces that are needed to enable the monitoring and configuration of security controls. This may lead to a lack of governance and control of compliance posture and increase the risk related to a large non-compliance time window.

Challenge 3: Synchronization between security orchestration and service orchestration

To maintain and enforce the right level of security compliance, security management needs to work in tandem with service management and orchestration (known as MANO). For instance, if security-relevant configurations (for example, network topology) are changed without coordination with the security management and orchestration system, the security posture of the whole environment may weaken. Also, if MANO is trying to configure a component that is non-compliant with established security policies while the security management system is trying to enforce the new security policies, this can result in conflict and increase the risk of a security breach.

Automated security compliance for operational assurance

To address the above mentioned challenges, there is a need for an automated security compliance management approach that encompasses monitoring, verification, orchestration, and enforcement of security compliance to increase auditability and maintain end-to-end compliance across different layers (for example, the virtual layer) and across different domains in a cloud based dynamic environment. This section describes the main set of capabilities and key features for implementing such a framework.

Security compliance frameworks and models

One of the main pillars for security compliance is defining the applicable compliance model and framework. A one-size-fits-all approach should be avoided, and instead, security controls should be combined to address different needs while discarding the overlapping ones (unless mandated by a specific security policy).

In this approach, several security models are of high importance. The zero-trust architecture (ZTA) model mandates that no implicit trust is assumed and that risks to assets and business functions are continuously assessed [7]. In addition to NESAS as described before, the NIST cybersecurity framework [8] is used to adapt ZTA to mitigate risks by enforcing appropriate controls according to updated security policies. The security compliance framework should as well follow the Cloud Security Alliance (CSA) Star approach [9] to continuously monitor and assess the compliance of security controls implemented based on ZTA with respect to the specified security policies.
Finally, considering privacy regulations (example the General Data Protection Regulation - GDPR), security compliance management solution must be realized in compliance with relevant privacy regulatory requirements.

Five key features for security compliance in NFV environments

To address the aforementioned challenges as well as privacy requirement, we foresee five key features as illustrated in Figure 3. Table 1 relates the key features to the aforementioned challenges and other requirements, where generally more than one key feature is needed to address a given challenge. In a nutshell, to achieve full stack end-to-end security compliance in NFV environments, the solution should be realized with adaptability and scalability in mind while preserving the privacy of tenants and users. Additionally, security compliance solution needs to implement a security compliance orchestration while handling multiparty compliance and offering a continuous proactive compliance approach.

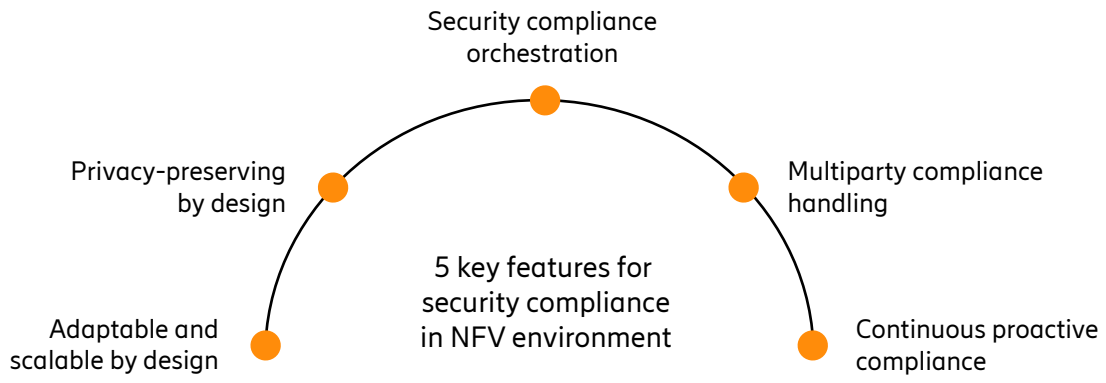

Figure 3. Five key features for security compliance in NFV environments

Key features	Challenges and requirements
Adaptable and scalable by design	Challenge 1, Challenge 2
Security compliance orchestration	Challenge 1, Challenge 2, Challenge 3
Multiparty compliance handling	Challenge 1
Continuous proactive compliance	Challenge 1, Challenge 2,
Privacy-preserving by design	Privacy regulatory requirements

Table 1. Relating the five key features to the aforementioned challenges and privacy regulatory requirements.

Adaptable and scalable by design

5G networks build on the capabilities of NFV to automatically scale resources and workloads based on load and performance requirements. Thus, security compliance mechanisms such as data logging, monitoring, and verification should be designed with the ability to scale in tandem to follow the dynamic and large-scale environment of 5G network services. Furthermore, standard monitoring interfaces should be defined to support secure control and programmability to allow adaptability of these mechanism to the ever-evolving security context. Moreover, novel algorithms should be developed to efficiently program these interfaces and control the content and frequency of the generated data to meet data accuracy objectives while minimizing the impact on the overall performance of the system.

Security compliance orchestration

5G networks and beyond are deployed across distributed administrative domains vertically encompassing several layers of the stack and horizontally linking the mobile users to the new services. Additionally, these mobile users can benefit from different types of services deployed at different network slices with different security requirements. To achieve full stack and end-to-end security compliance for different slices, security compliance management needs to adapt to the changing security context (related to the service slice or to the administrative domain) while preserving the same level of security protection and risk control. This can be achieved by adapting the orchestration feature inherent in the NFV environment to orchestrate security compliance as well. Moreover, orchestrating security compliance across layers and domains would require dealing with significantly large-scale data and collaborations involving privacy issues. To address this issue, artificial intelligence-based automation such as federated learning can be utilized.

Multiparty compliance handling

Different stakeholders (that is, NFVI providers, network function vendors, service providers) are involved in delivering and managing different components of the telecom environment. As the state of any component in the NFV environment maps into different layers, and those layers may be controlled by different administrative domains, their compliance involves a shared responsibility between stakeholders. For example, when it comes to verifying the access control compliance for a network function instance, different security compliance checks might be required from the NFVI provider (for example, computing and networking isolation between different customers) and the customer or service provider

deploying the virtual network functions (application layer control). To monitor and verify the compliance, trust between different stakeholders needs to be established to ensure that each party has adequately covered its part of the responsibility. Therefore, there is a need to develop multiparty compliance approaches to build trust among these different stakeholders, and efficiently combine the per layer or per domain compliance results into a reliable assessment of the compliance of different components. In this context, standardization will play an important and possibly an accelerator role.

Furthermore, this multi-party compliance affects the way the evidence for the compliance is collected and presented (for example, for proving a possible breach) to the tenants. An evidence-based compliance approach toward the tenants necessitates that the proof of compliance would be available to them. For example, the compliance verification of a network slice isolation may require the aggregation of the logs at different layers from multiple network slices from different tenant network slices shared among different administrative domains in the cloud or virtualized environment. Additionally, the required logs could be the composition of disaggregated logs from multiple domains and the logs from per slice specific logging and monitoring components. New mechanisms, then, are needed to collect and aggregate the right traces at the right time for different tenants, at different layers under different administrative domains (for example, the hyperscale cloud provider) and anonymize them without removing important correlation relations between the traces from different layers and domains before providing them to the tenants.

Continuous proactive compliance

The dynamic runtime modifications to the virtual infrastructure and its configuration brought by NFV and SDN may cause changes to the security compliance status and therefore, logging and monitoring mechanisms should adapt to continuously monitor compliance-related events and metrics and verify the security posture after relevant events. New approaches must be conceived to adapt to the rate of change and lessen the burden of verifying compliance from scratch between the successive changes around virtualized infrastructure. Event-based approaches can be considered to trigger compliance verification in time, while the proactive techniques that leverage machine learning may enable efficient identification and advance checking of system changes to minimize delays and overhead.

Privacy-preserving by design

Security logging and monitoring mechanisms should not introduce additional risks to the security and the privacy of data through the 5G networks. While current anonymization approaches help in protecting data, general attributes and semantics of the data are not preserved, which may mean it is impossible to effectively analyze the data. Therefore, there is a need for new customizable and flexible anonymization and privacy-preserving approaches that correctly protect data across different domains and different network slices while preserving the utility of the data for different types of analysis.

Conclusion

Evolving telecom networks call for an evolved security compliance framework for a securely connected world. This white paper demonstrated the need for an automated full-stack end-to-end security compliance solution and the challenges that have to be overcome to realize it. Five key features were described that support such a solution. This solution should be realized with a focus on adaptability, scalability and privacy-enhanced technology while providing continuous proactive security, multi-party compliance, and security compliance orchestration. These key features are supported by monitoring, verification, and enforcement mechanisms integrated into the network function virtualization environment.

For such a solution, telecommunication organizations should evolve operational security assurance in addition to product security assurance. The telecom community including vendors, regulators, and service providers should increase their collaborative work to reduce the complexity in terms of responsibility between stakeholders operating the NFV stack from the CI/CD (developers, telecom vendors) to the deployment (service providers and infra providers). Service providers should move toward more automated and continuous security compliance of NFV to provide up-to-date compliance posture visibility to tenants and allow them to have better control of compliance enforcement for their deployments. Finally, standard 5G network interfaces for facilitating security compliance automation should be defined to ensure a coordinated service and security orchestration.

Glossary

5G	Fifth generation
3GPP	The 3rd Generation Partnership Project
CSA	Cloud Security Alliance
ETSI	European Telecommunications Standards Institute
GSMA	Global System for Mobile Communications Association
MANO	Management and Orchestration
NESAS	Network Equipment Security Assurance Scheme
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NIST	National Institute of Standards and Technology
SDN	Software-defined networking

References

1. ENISA, NFV Security in 5G - Challenges and Best Practices, https://www.enisa.europa.eu/publications/nfv-security-in-5g-challenges-and-best-practices
2. NIST, Security and Privacy Controls for Information Systems and Organizations, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf
3. NESAS framework, https://www.gsma.com/security/wp-content/uploads/2022/02/FS.13-v2.1.pdf
4. Ericsson Cloud RAN passes GSMA's NESAS security audit. https://www.ericsson.com/en/news/2022/1/ericsson-cloud-ran-passes-gsmas-nesas-security-audit
5. Ericsson 5G Core and transport technologies fully compliant with 3GPP/GSMA NESAS security standards. https://www.ericsson.com/en/news/2021/2/5g-core-and-transport-is-3gpp-gsma-nesas-security-compliant
6. ETSI, Security Assurance Profile for Secured Telecommunications Operations; Statement of needs for security assurance measurement in operational telecom infrastructures. TR 187 023 V1.1.1 (2012-03)https://www.etsi.org/deliver/etsi_tr/187000_187099/187023/01.01.01_60/tr_187023v010101p.pdf
7. NIST, Zero Trust Architecture, SP 800-207, August 2020, https://csrc.nist.gov/publications/detail/sp/800-207/final
8. NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
9. Cloud Security Alliance (CSA), STAR Program & Open Certification Framework in 2016 and beyond, April 2016
10. Microsoft, Operational security for online services overview, https://download.microsoft.com/download/9/D/B/9DBA2020-5E81-4A54-8C5D-4938B0FAE042/Operational-Security-for-Online-Services-Overview.pdf

Further reading

1. https://www.ericsson.com/en/blog/2022/2/demystifying-the-key-benefits-of-network-security-automation
2. https://www.ericsson.com/en/news/2021/2/5g-core-and-transport-is-3gpp-gsma-nesas-security-compliant

Authors

Yosr Jarraya is a Master Researcher in Security with Ericsson Research. Prior to joining Ericsson in 2016, she had a two-year postdoctoral fellowship with the company. She is an engineer and holds a Ph.D. in electrical and computer engineering from Concordia University in Montreal. She has several patents granted or pending. She has also co-authored 2 books and several research papers in scientific journals and conferences on the topics of security of software, NFV, SDN and cloud.

Ari Pietikäinen is a senior security specialist. He joined Ericsson in 1990 and has worked in the security domain since 2003, most recently with cloud, NFV and IoT security topics. He holds an M.Sc. from Helsinki University of Technology in Espoo, Finland.

Jukka Ylitalo is a Principal Researcher in Security with Ericsson Research. Jukka holds M.Sc. and D.Sc. (Tech.) from Helsinki University of Technology, Finland. He has been working at Ericsson research and different business units in several roles for twenty years and headed R&D in a start-up company earlier in his career. He has published scientific articles in the field of security and mobility, contributed to security standardization and has several granted patents. Jukka is currently working on 6G system security design.

Giovanni Zanetti is actually "Head of Security Delivery" in Mediterranean and Latin America" market area at Ericsson. His expertise includes general Security knowledge on TELCO and Enterprise architecture with a focus on 5G and NFVi Security, and all the audit and risk management areas. His activities have focus on customer's security and how implement and harmonize the security at best level. Currently work on a Security Training program for Customer's managers/executive on 5G Security. He contributes on several conferences for Ericsson and ISSA, security association.

Jonathan Olsson is an Expert in RAN Security Architecture. He joined Ericsson in 2004 as a researcher for fixed access networks. Since then, he has had roles held several security roles across different organizations within Ericsson. In his current role, Olsson drives technology strategy and exploratory security research in RAN. He has a B.Sc. in computer science from Uppsala University, Sweden, and is a Certified Information Systems Security Professional.

Dr. Makan Pourzandi is a research leader at the research department, Ericsson, Canada. He received his Ph.D. degree in Computer Science from University of Lyon I Claude Bernard, France and M.Sc. in parallel computing from École Normale Supérieure de Lyon, France. He has more than 20 years of experience in the fields of cyber security, Telecom and distributed systems. He co-authored two books on cyber security published by Springer on auditing in cloud environments and software security. He is the co-inventor of 25 granted US patents. He has published more than 80 research papers in peer-reviewed scientific journals and conferences. His current research interests include cyber security, cloud computing, software security engineering.