



Thematic reference framework — CYBERSECURITY domain

1. Cryptography

Scope

This theme covers the whole range of cryptographic primitives, protocols and mechanisms used to ensure the confidentiality, integrity, authenticity and non-repudiation of data and communications. It encompasses both the design of algorithms and the formal verification of their security and of their implementation, as well as the lifecycle management of cryptographic keys and parameters. It cuts across all the other themes, in that it constitutes the foundation of trust on which system protection mechanisms rest.

Sub-topics

- Post-quantum cryptography
- Automatic and semi-automatic security proofs of cryptographic protocols
- Security of cryptographic implementations
- New cryptographic services
- Formalising the verification of the proper management and use of cryptographic algorithms, parameters and keys within a product or a system
- Modelling of known randomness sources, assessment of the quality of randomness

2. Component security

Scope

This theme addresses the security of low-level hardware and software components — microprocessors, integrated circuits, firmware, embedded systems — considered as elements of trust within a security chain. It deals with the mechanisms that harden these components against physical or logical attacks, with the assessment of their robustness through hardware evaluation techniques (side channels, fault injection), and with the formal verification of the soundness of their design.

Sub-topics

- Mechanisms for securing components
- Techniques for assessing the robustness of components against side-channel attacks, direct observation or fault injection
- Specification, formalisation and verification of the secure design of hardware and software architectures — hardware aspects

3. Wireless transmission security (low-level protocols, TEMPEST, communications, attacks and vulnerabilities that may compromise radio, Wi-Fi and Li-Fi links)

Scope

This theme addresses the threats and protection mechanisms specific to wireless transmissions: unintentional electromagnetic emissions (TEMPEST), vulnerabilities of radio protocols and RF chains (Wi-Fi, Li-Fi, LoRa, 5G/6G), and the convergence between cybersecurity and electronic warfare. It covers both passive attacks (interception, observation) and active ones (jamming, spoofing, injection) targeting wireless communication equipment.

Sub-topics

- Attacks and vulnerabilities that may compromise the security of radio communications
- Analysis of the convergence between cyber and electronic-warfare attack methods
- Security of multi-protocol MESH network architectures (LoRa, Starlink, 5G, 6G, etc.)

4. Network security (stealth, network protocols, protocol hardening)

Scope

This theme deals with the security of network infrastructures and communication protocols: hardening of existing protocols, network intrusion detection, adaptive monitoring, and secure architectures for enterprise networks and industrial systems. It also includes network stealth techniques and the mechanisms that make it possible to detect malicious traffic, in particular in the presence of encryption.

Sub-topics

- Adaptive monitoring of network security based on knowledge of the threat and of the environment
- Data-centric security systems
- Detection in the presence of encrypted traffic
- Visualisation techniques for security monitoring

5. Security of the low-level software layers

Scope

This theme addresses the security of the software layers closest to the hardware: operating systems, hypervisors, virtualisation mechanisms, firmware and trusted execution environments. It encompasses both the secure design of these layers and their hardening against attacks, and covers the formal specification of sound software architectures at this level of abstraction.

Sub-topics

- Mechanisms for securing operating systems and virtualisation mechanisms
- Specification, formalisation and verification of the secure design of hardware and software architectures — low-level software aspects

6. Application security (upper software layers, web security, databases)

Scope

This theme covers the security of applications and of application-level software systems: web applications, APIs, databases, middleware, cloud services. It includes secure development techniques, the search for vulnerabilities in source code or binaries, and application penetration testing. It is closely linked to the « Languages and software engineering » theme, of which it constitutes the applied field oriented towards the detection of flaws.

Sub-topics

- Static and dynamic code analysis techniques, search for vulnerabilities in source code or binaries
- Large-scale automated AI-based code analysis

- Automation of penetration testing
- Security of cloud architectures

7. Languages, software and binary engineering

Scope

This theme encompasses security-oriented software engineering methods and tools: formal languages, verification methods, program analysis (static, dynamic, symbolic), automatic code generation and evaluation, fuzzing, software dependency management, obfuscation and diversification techniques, and the automatic construction of knowledge graphs associated with a piece of code. It provides the common technical foundation for application security, malware analysis and vulnerability research.

Sub-topics

- Static and dynamic code analysis techniques, search for vulnerabilities in source code or binaries
- Large-scale automated AI-based code analysis, vulnerability research
- Automated binary analysis, including similarity search
- Specification, formalisation and verification of secure architecture design — formal methods aspects

8. Hardware architecture (specification, formalisation, verification, CPU/GPU and RAM/VRAM hybridisation, ARM and RISC-V threats)

Scope

This theme addresses the design and evaluation of hardware architectures from a security standpoint: processors (ARM, RISC-V, x86), memories, heterogeneity and CPU/GPU and RAM/VRAM hybridisation, and their specific attack surfaces. It includes the formalisation of the security properties expected of an architecture and their verification, as well as the threats specific to new platforms (micro-architectural side channels, hardware supply-chain attacks). It also covers the security of the hardware infrastructure associated with large-scale hosting.

Sub-topics

- Specification, formalisation and verification of the secure design of hardware architectures — hardware aspects
- Attacks and vulnerabilities that may compromise information systems — hardware platform aspects
- Security of hardware infrastructure (NAS, immutable storage arrays, SAN, remote management cards, building management systems, etc.)
- Vertical logical stacking architectures (large-scale integration strategy)

9. Software architecture (specification, formalisation and verification of secure design)

Scope

This theme covers the sound design of complex software systems: definition of security architectures, privilege separation, access control models, and formal verification of the security properties of software architectures. It complements the « Languages and software engineering » theme by focusing on the architectural level rather than on the code level.

Sub-topics

- Specification, formalisation and verification of software — software aspects

- Mechanisms for securing operating systems and virtualisation — architectural design aspects
- Security of cloud architectures

10. Security of IT and OT/IoT systems (detection, monitoring, human-machine interfaces, decision support, embedded AI)

Scope

This theme is the most transverse: it covers the security of information systems in their operational entirety, including industrial systems and the IoT. It brings together intrusion detection, security monitoring, decision support and human factors. It constitutes the level of integration above the technical layers, where incident response is managed and where the defensive posture is built. Threat knowledge and cyber intelligence fall under theme 13.

Sub-topics

- Data-centric security systems
- Adaptive monitoring of network security based on knowledge of the threat
- Security of industrial control systems and OT
- Detection of malware and of advanced attacks
- Big-data processing to detect abnormal behaviour and weak signals of attack
- Decoy and bait techniques to mislead or divert the attacker
- Optimisation of defence strategies
- Evaluation of detection solutions
- Visualisation techniques for security monitoring

11. Social engineering for cyber (communities, fakes, social bots, etc.)

Scope

This theme covers the human and social dimensions of the cyber threat, in particular influence and manipulation operations exploiting social networks, digital media and human behaviour. It encompasses the detection of disinformation and deepfakes, the behavioural analysis of online communities, stylometry, the attribution of influence operations and counter-narrative capabilities. It corresponds to « Lutte Informatique d'Influence » (L2I) in the orientation document.

Sub-topics

- Analysis and characterisation of communities
- Fake detection: altered content and deepfakes — text, images, audio, video
- Detection of social bots and of coordinated behaviour
- Author profiling, stylometry — multimodal style recognition
- Analysis of opinions, emotions and sentiment, and of their evolution and propagation
- Topic modelling, extraction of narrative elements, narrative evolution, topic threading
- Possibly multimodal information extraction: entities, events
- Support for building argumentation or counter-argumentation
- Analysis of the impact of influence operations, characterisation of the effects produced

12. Cybersecurity of AI (protection, hardening, monitoring of AI-based systems)

Scope

This theme deals with the security of systems incorporating artificial intelligence, on the one hand as a target of attacks (adversarial attacks, data poisoning, model theft, evasion) and on the other as a vector or amplifier of attacks. It also includes explainability as a prerequisite for trust in AI

systems used for defence purposes, the detection of unauthorised embedded AI models, and the measurement and monitoring of the quality of model training.

Sub-topics

- Bias in AI models: detection, reinforcement and exploitation of such bias, poisoning (CREACH LABS addition)
- Security of agentic systems and self-improvement (CREACH LABS addition)
- Secure integration into systems (CREACH LABS addition)
- Detection of unauthorised embedded AI models

13. Threat knowledge

Scope

This theme brings together work on understanding and characterising attackers, their modes of operation and their technical capabilities. It covers cyber intelligence, the analysis of offensive techniques (exploitation of vulnerabilities, circumvention of defences), attribution methods, and the formalisation of knowledge about threats (ontologies, knowledge bases). It is essential to all the fields of engagement.

Sub-topics

- Attacks and vulnerabilities that may compromise the security of information systems
- Methods for circumventing security solutions
- Techniques for detecting the circumvention of detection solutions
- Methods and means of attack attribution
- Big-data processing for the analysis of attack methods and for cyber intelligence
- Knowledge building and management — ontologies
- Attack methods employing artificial intelligence techniques