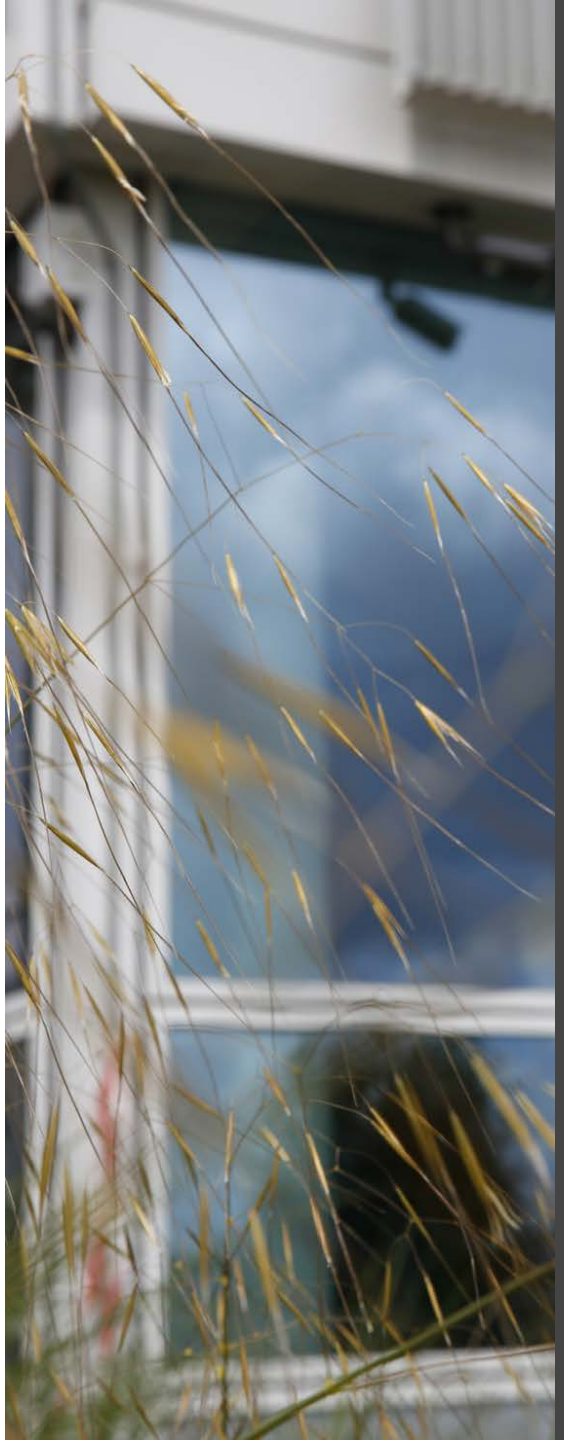
INNOVATIVE AND OPERATIONAL APPROACHES TO CYBERSECURITY

Active involvement in Research & Innovation agendas

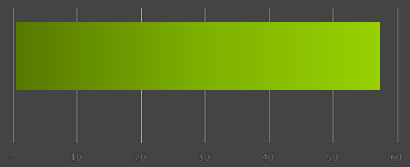
Cybersecurity as a multi-disciplinary program

Wide-ranging operational expertise



CYBERSECURITY

A research excellence powered by operational challenges



190+ scientists
3 Operational Divisions
15 coordinated teams

Involvement in local, national, European and international collaborations

Contributions range across

- Security in hardware
- Formal methods and theory of security and privacy
- Cryptology design, techniques and protocols
- Software and application security
- Systems security
- Intrusion/anomaly detection and malware mitigation
- Network security
- Database and storage security and privacy
- Forensics

Analyze systems and characterize the threats

Secure systems through patented HW/SW technologies

Security evaluation tools and capabilities (ITSEF)

CYBERSECURITY PLATFORM

Mission

- **Identify product vulnerabilities**
- **Develop innovative ways to protect both hardware and software from cyber-attacks.**

An world unique innovation ecosystem to secure by design critical functions

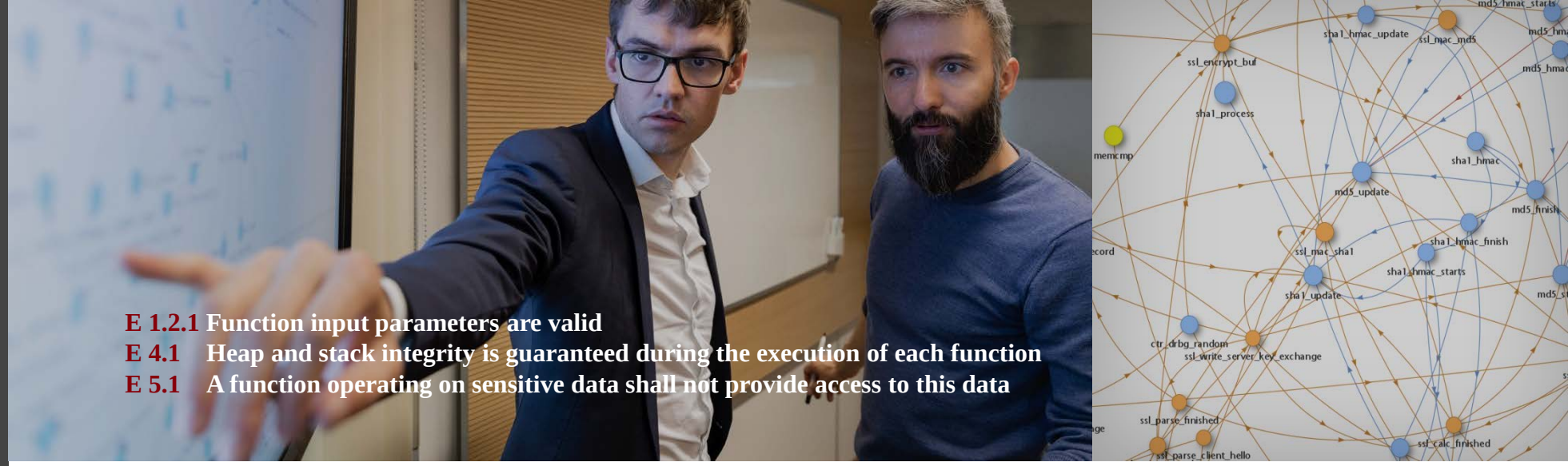
- State-of-the art benches & tools
- A large patents portfolio
- Long time collaboration with academics and stakeholders

Research focus

- Attacks benches
- Security assessment and verification tools
- Hardware & software root of trust
- Disruptive technologies for cybersecurity

Teams in Grenoble, Paris, Toulouse & Gardanne

ADVANCED SOFTWARE ANALYSES



Cyber-attacks largely rely on software flaws. Software trust is becoming a cornerstone of business requirements and normative compliance

NEXT-GENERATION AUDITING

Traditional techniques rely on reviews and tests to try to find flaws faster than attackers do

RECOGNIZED GUARANTEES

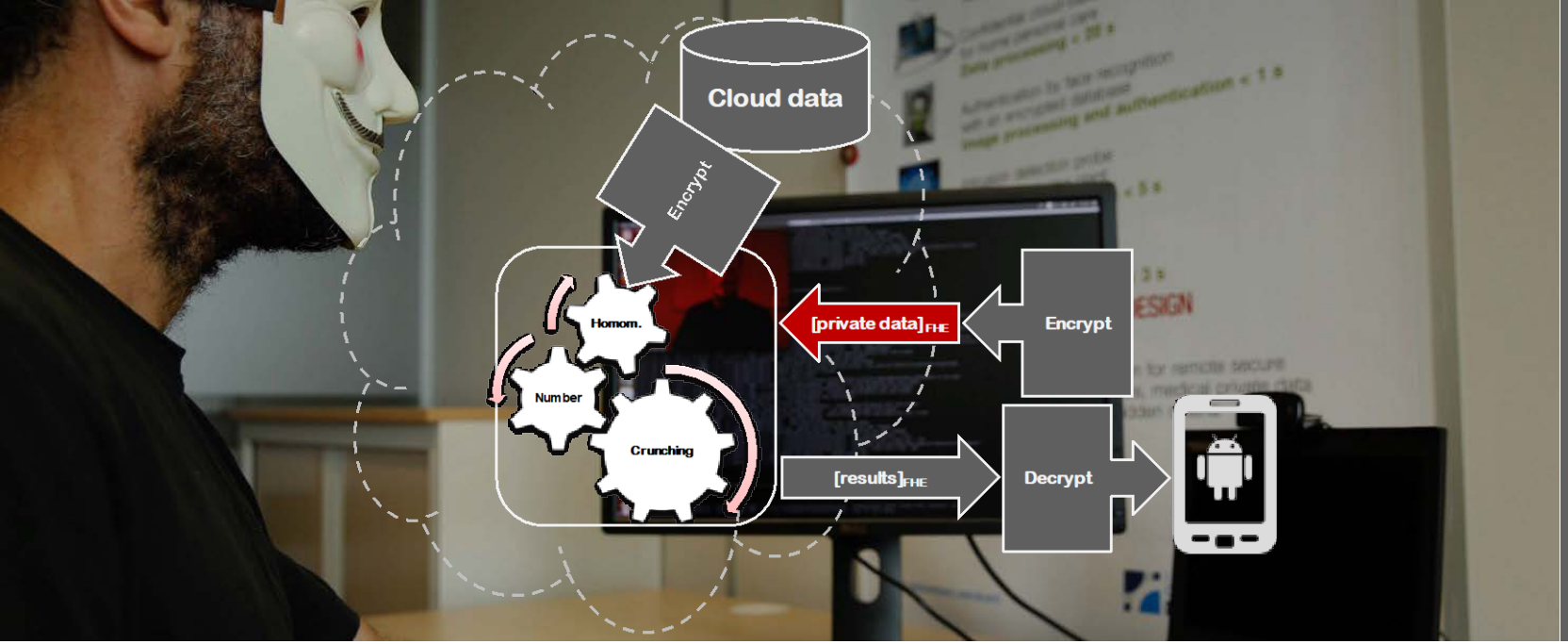
The world's first tool to pass NIST's Ockham Criteria for the exhaustive detection of common security flaws

FRAMA-C AND BINSEC

Automated analysis platforms based on advanced reasoning, providing mathematics-backed security proofs

INDUSTRIAL IMPACT

CEA's software analysis platforms are used across CEA, and by teams from DGA, Airbus, Dassault and Thales



ENABLING CRYPTO-COMPUTING

Fully homomorphic encryption is a mathematical breakthrough that allows computations to occur on cyphered data, protecting information from end to end

ENCRYPTION FOR ALL

Help software developers integrate homomorphic encryption techniques in their apps. Optimize the performance of these operations

CINGULATA

The leading compilation toolchain is developed at List, allowing engineers to optimize and deploy homomorphic cryptography in real-world applications

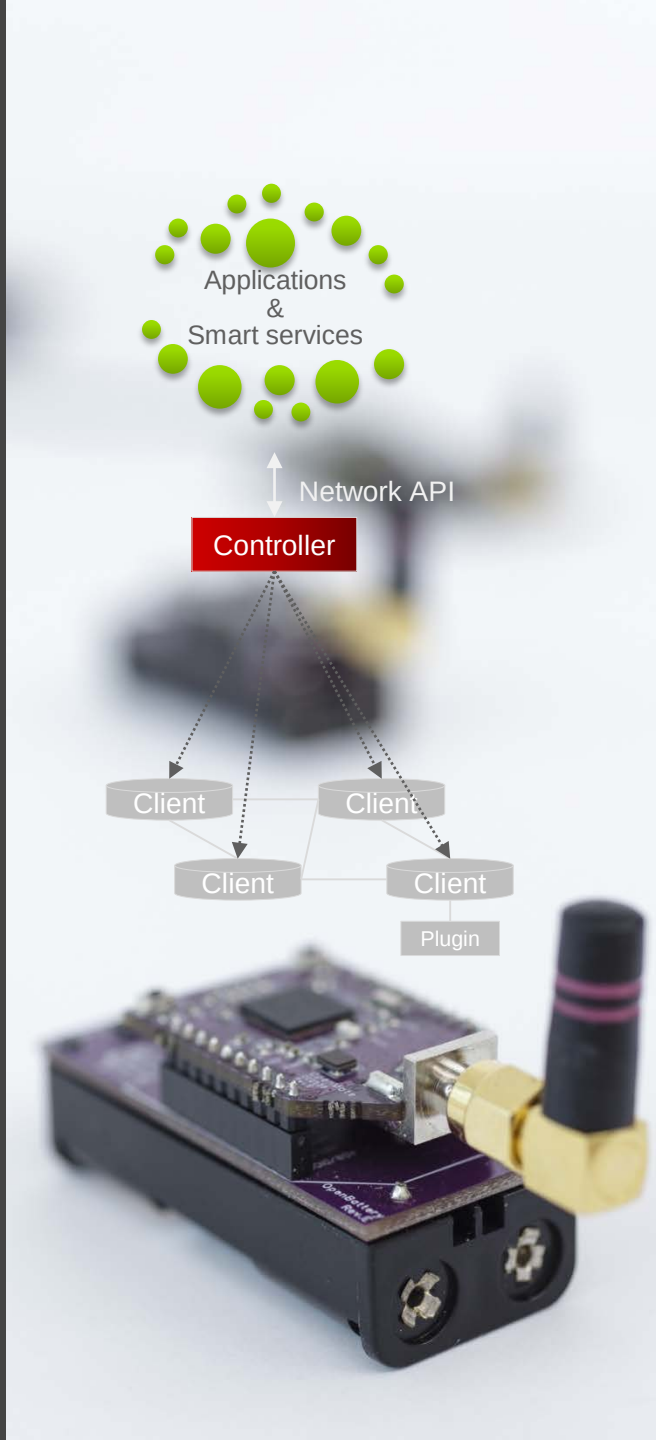
COMPATIBLE TODAY

Teams at List have breached sub-second trans-cyphering capabilities, an essential step for homomorphic deployments to interoperate with legacy environments

list
cea tech

COGNITIVE NETWORK SECURITY

Reactive network tactics are becoming a key component of cybersecurity strategies, both in IT systems and more constrained IoT deployments



FASTER REACTION TIMES

Integrate machine learning and optimization techniques to detect anomalies, and propose counter-measures

NEON

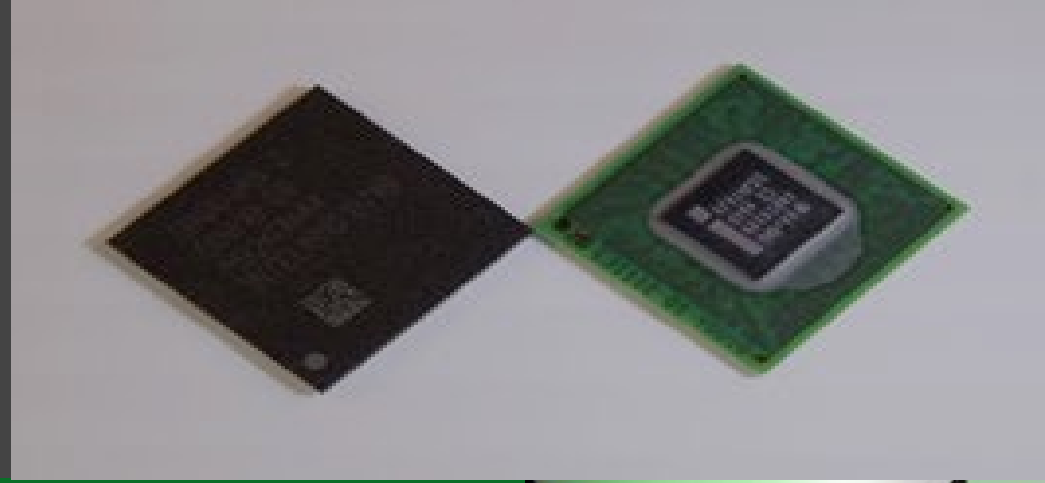
Extend SDN controls to enable virtualized network security functions and implement cognitive security in heterogeneous communication systems

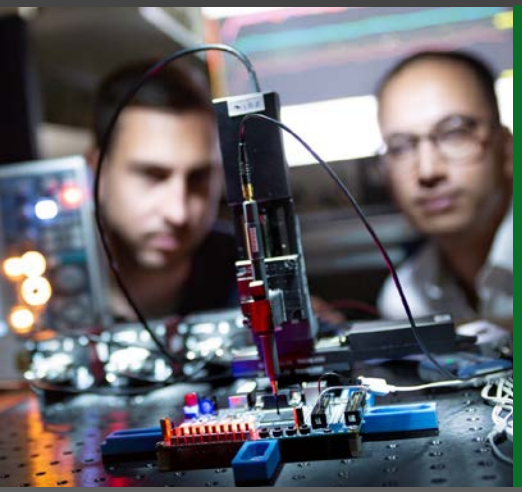
INTELLIGENT RECONFIGURATION

Teams at List have pioneered the use of genetic algorithms for autonomous management of a distributed network intrusion detection system

LIFECYCLE SECURITY

Evolution of the security requirements of architecture, equipment, connections along the hardware lifecycle
Authenticity, integrity, updates





WORLD-CLASS HARDWARE BENCHES

Attacks on IC: physical, fault injection, side-channels, trojans.
Counter-measure evaluation
Hardware monitoring of software attacks

EXTENSIVE EVALUATION EXPERTISE

Assisting the specification of security requirements
Helping providers secure and evaluate their products
Preparing for certification