BIBLIOGRAPHIE

Guides de bonnes pratiques

• *Recommandations de sécurité pour la journalisation des systèmes Microsoft Windows en environnement Active Directory,* guide technique, version 1.1.
En savoir plus

• *Recommandations de sécurité pour l'architecture d'un système de journalisation*, guide technique, version 2.0.
En savoir plus

• *Recommandations de configuration des commutateurs et pare-feux Hirshmann*, guide technique, version 1.3.
En savoir plus

• *Recommandations de configuration des commutateurs et pare-feux Siemens Scalance,* guide technique, version initiale.
En savoir plus

• *Recommandations de configuration d'un système GNU/Linux*, version 2.0.
En savoir plus

• *La cybersécurité pour les TPE/PME en treize questions*, version 2.0.
En savoir plus

• *10 règles d'or pour la conception et la mise en œuvre de services numériques.*
En savoir plus

Partenariats

• ANSSI-Afpa, *L'attractivité et la représentation des métiers de la cybersécurité*, novembre 2022.
En savoir plus

Publications scientifiques

Laboratoire architecture matérielle et logicielle (LAM)

User-friendly Lightweight TPM Remote Attestation over Bluetooth, **Loïc Buckwell**, **Nicolas Bouchinet** et **Gabriel Kerneis**, OSFC 2022.

Laboratoire cryptologie (LCR)

Secure storage - Confidentiality and authentication, **Ryad Benadjila**, **Louiza Khati**, Damien Vergnaud, *Computer Science Review* vol. 44: 100465 (2022).

Mitaka : a simpler, parallelizable, maskable variant of Falcon, Thomas Espitau, Pierre-Alain Fouque, François Gérard, **Mélissa Rossi**, Akira Takahashi, Mehdi Tibouchi, Alexandre Wallet and Yang Yu, *Proceedings of Eurocrypt* 2022 (3), pp. 222-253, Springer 2022.

Chapitre *"Differential Cryptanalysis, Symmetric Cryptology – Book 2"*, **Henri Gilbert**, **Jérémy Jean**, pp. 3-28, *Encyclopedia Sciences*, ISTE-WILEY.

Generic attack on Duplex-based AEAD modes, **Henri Gilbert**, Rachelle Heim Boissier, **Louiza Khati**, Yann Rotella, Frisiacrypt 2022.

The Hidden Parallelepiped Is Back Again: Power Analysis Attacks on Falcon, Morgane Guerreau, **Ange Martinelli**, Thomas Ricosset and **Mélissa Rossi**, TCHES 2022 (3), pp. 141-164 (2022).

Sécurité étendue de la cryptographie fondée sur les réseaux euclidiens : tour d'horizon des techniques d'attaque et de protection, **Mélissa Rossi**, présentation sur invitation, Journées C2, Hendaye, 13 avril 2022.

Side-channel countermeasures for lattice-based cryptography, **Mélissa Rossi**, VeriSiCC Seminar, Paris, 22 septembre 2022.

Chapitre *"H-Coefficients Technique, Symmetric Cryptology – Book 1"*, **Yannick Seurin**, pp. 173-184, *Encyclopedia Sciences*, ISTE-WILEY.

Interactive Oracle Proofs of Proximity to Algebraic Geometry Codes, Sarah Bordage, Mathieu Lhotel, Jade Nardi, **Hugues Randriam**, *Computational Cryptography Conference* 2022, 30:1-30:45, 2022.

Laboratoire exploration et recherche en détection (LED)

Multilayer block models for exploratory analysis of computer event logs, Corentin Larroche, CAN, 2022 *Proceedings*.

Side Channel Analysis against the ANSSI's protected AES implementation on ARM, Loïc Masure et **Rémi Strullu**, JCEN, 2022.

Security Assessment of NTRU Against Non-Profiled SCA, Luk Bettale, Julien Eynard, Simon Montoya, **Guénaël Renault** et **Rémi Strullu**. CARDIS, 2022.

Laboratoire sécurité des composants (LSC)

A Finer-Grain Analysis of the Leakage (non) Resilience of OCB, Francesco Berti, Shivam Bhasin, Jakub Breier, Xiaolu Hou, **Romain Poussier**, François-Xavier Standaert et Balazs Udvarhelvi. IACR *Transactions on Cryptographic Hardware and Embedded Systems*, Volume 2022, number 1, 2022.

Security Assessment of NTRU Against Non-Profiled SCA, Luk Bettale, Julien Eynard, Simon Montoya, **Guénaël Renault** et **Rémi Strullu**. CARDIS, 2022.

Fault injection effectiveness compared to reflection coefficient of antenna/target couple, **Guillaume Bouffard**, **Valentin Houchouas**, **José Lopes-Esteves** et **Thomas Trouchkine**. 3rd URSI AT-AP-RASC, 2022.

Building a Commit-level Dataset of Real-world Vulnerabilities, Alexis Challande, Robin David et **Guénaël Renault**. CODASPY, 2022.

L'attaque en faute : la bête noire des boîtes blanches, Vincent Giraud et **Guillaume Bouffard**. JAIF, 2022.

Practical timing and SEMA on embedded OpenSSL's ECDSA, Adrian Thillard, **Franck Rondepierre**, **Guénaël Renault** et **Julien Eynard**. SSTIC, 2022.

Laboratoire de la sécurité des technologies sans-fil (LSF)

Fault injection effectiveness compared to reflection coefficient of antenna/target couple, **Guillaume Bouffard**, **Valentin Houchouas**, **José Lopes-Esteves** et **Thomas Trouchkine**. 3rd URSI AT-AP-RASC, 2022.

Implantation d'information dans des cibles non coopératives : application à la lutte anti-drone, **José Lopes Esteves**, 2022, 8e journées d'étude électromagnétisme et guerre électronique (EM+GE), ONERA.

Comparing Intentional Electromagnetic Interference and Electromagnetic Fault Injection for electromagnetic security applications, **José Lopes Esteves**, 2022, URSI.

Laboratoire Sécurité du logiciel (LSL)

A Bottom-Up Formal Verification Approach for Common Criteria Certification: Application to JavaCard Virtual Machine, Adel Djoudi, Martin Hana, Nikolai Kosmatov, Milan Krızenecky, Franck Ohayon, **Patricia Mouy**, **Arnaud Fontaine** et David Feliot, ERTS 2022, ***Best paper award.***

Le temps des cerises : efficient temporal stack safety on capability machines using directed capabilities, Linn Georges, **Alix Trieu** et Lars Birkedal, OOPSLA, 2022, ***Distinguished paper award.***

Publications open source

Laboratoire architecture matérielle et logicielle (LAM)

Maintien (continu) de linux-hardened, un *patchset* de durcissement du noyau Linux notoirement utilisé par la distribution Android durcie GrapheneOS et d'autres distributions Linux tel que Archlinux.

Keysas, a USB virus cleaning station
Code source Gitlab
Documentation

Ultrablue: a remote attestation server for your phone
Code source Github

Patch (PR #486) d'intégration de Landlock dans Linux PAM, qui doit permettre de restreindre la vue du système aux processus privilégiés de PAM, par exemple unix_chkpwd.

Laboratoire sécurité réseau, protocole (LRP) et Laboratoire Sécurité du logiciel (LSL)

Parser x.509 : mise à jour avec l'ajout du support des CRLs, migration vers la nouvelle version de FRAMA-C.

Rapport sur les incidents et menaces

• *Panorama de la cybermenace 2021.*
En savoir plus

• *Vulnérabilité dans Atlassian Confluence. CERT-FR. 6 juin 2022.*
En savoir plus

• *Menaces liées aux vols de cookies et contre-mesures. CERT-FR. 25 mai 2022.*
En savoir plus

Référentiels

• *SecNumCloud, version 3.2.*
En savoir plus

Référentiel d'exigences applicables aux prestataires d'administration et de maintenance sécurisées (PAMS), version 1.1 du 6 octobre 2022.
En savoir plus

Référentiel d'exigences applicables aux prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS),version 0.3.2 du 17 octobre 2022
En savoir plus

Légende

(EN) : également disponible en anglais

Noms en gras : personnes rattachées à l'ANSSI au moment de la soumission ou de la publication de l'article scientifique.