RAPPORT D'ACTIVITÉ

2023 BIBLIOGRAPHIE

GUIDES DE BONNES PRATIQUES

Les Essentiels

Sauvegarde des systèmes d'information, version 1.1.
En savoir plus

Les dénis de services distribués (DDoS), version 1.1.
En savoir plus

Mise en œuvre sécurisée d'un CMS, version 1.1.
En savoir plus

Virtualisation, version 1.0.
En savoir plus

Les Fondamentaux

Sauvegarde des systèmes d'information, version 1.0.
En savoir plus

Les guides techniques

Recommandations relatives au reconditionnement des ordinateurs de bureau ou portables, version 1.0.
En savoir plus

Recommandations sur le nomadisme numérique, version 2.0.
En savoir plus

Recommandations relatives à l'administration sécurisée des SI reposant sur Microsoft Active Directory, version 1.0.
En savoir plus

Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection, version 2.1.
En savoir plus

Corpus documentaire IPsec DR à destination des industriels, version 1.0.
En savoir plus

Profil de protection pour les systèmes industriels, Les automates, version 1.2.
En savoir plus

ANSSI views on the Zero Trust model.
En savoir plus

Configuration recommendations of a GNU/LINUX system, version 2.0.
En savoir plus

Les kits d'exercice de crise sectoriels

Kit d'exercice dédié aux collectivités territoriales

Kit d'exercice dédié au secteur de l'Enseignement supérieur et de la Recherche

Kit d'exercice dédié au contexte des Jeux Olympiques et Paralympiques 2024

En savoir plus

PUBLICATIONS SCIENTIFIQUES

Thèse de doctorat

Laboratoire de la sécurité des technologies sans-fil

J. Lopes Esteves, « Electromagnetic Interference and Information Security: Characterization, Exploitation and Forensic Analysis. » PhD Thesis, HESAM Université, 2023.
En savoir plus

Laboratoire exploration et recherche en détection

C. Larroche, « A source separation approach to temporal graph modelling for computer networks », MLCS 2023 (ECML workshop).
En savoir plus

L. Aubard, **J. Mazel**, G. Guette, **P. Chifflier**, O. Levillain, G. Blanc, L. Mé, « Modélisation et test des ambiguïtés de recouvrement de données pour l'obtention des politiques de réassemblage dans les protocoles réseaux », Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI), 2023.
En savoir plus

Laboratoire sécurité du logiciel

M. Baty, P. Wilke, G. Hiet, **A. Fontaine**, **A. Trieu**, « A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity », 2023 IEEE 36th Computer Security Foundations Symposium (CSF), Dubrovnik, Croatia, 2023, pp. 372-387.
En savoir plus

Laboratoire sécurité réseau, protocole

V. Cortier, P. Gaudry, S. Glondu, **S. Ruhault**, « French 2022 legislatives elections: a verifiability experiment », E-Vote-ID 2023.
En savoir plus

A. Ebalard, R. Benadjila, « Randomness of random in Cisco ASA », SSTIC 2023.
En savoir plus

Laboratoire architecture matérielle et logicielle

V. Giraud, **G. Bouffard**, « Faulting original mceliece's implementations is possible: How to mitigate this risk? », Symposium on Security and Privacy, EuroS&P 2023 -Workshops on the Security of Software/Hardware Interfaces (SILM), pages 311–319.
En savoir plus

Laboratoire sécurité des composants

S. Boussam, J. Eynard, **G. Renault**, G. Zaïd, « Étude critique d'une méthode de Machine Learning appliquée à l'analyse par canaux auxiliaires », SSTIC 2023.
En savoir plus

Articles scientifiques présentés en conférence

Laboratoire cryptologie

R. del Pino, T. Prest, **M. Rossi**, Markku-Juhani O. Saarinen, « High-Order Masking of Lattice Signatures in Quasilinear Time », Security & Privacy 2023.
En savoir plus

H. Gilbert, R. Heim Boissier, **L. Khati**, Y. Rotella, « Generic «Attack on Duplex-Based AEAD Modes Using Random Function Statistics », EUROCRYPT 2023, pp. 348-378.
En savoir plus

H. Beguinet, C. Chevalier, D. Pointcheval, T. Ricosset, **M. Rossi**, « GeT a CAKE: Generic Transformations from Key Encaspulation Mechanisms to Password Authenticated Key Exchanges », ACNS 2023, pp. 516-538.
En savoir plus

S. Agrawal, **M. Rossi**, S. Yamada, A. Yadav, « Constant Input Attribute Based (and Predicate) Encryption from Evasive and Tensor LWE », CRYPTO 2023, pp 532-564.
En savoir plus

M. Rossi, Markku-Juhani Saarinen, « Mask Compression: High-Order Masked Cryptography with Limited Memory », SAC 2023.
En savoir plus

H. Gilbert, R. Heim Boissier, **J. Jean, J-R. Reinhard**, « Cryptanalysis of Elisabeth-4 », ASIACRYPT 2023, pp. 256-284.
En savoir plus

R. del Pino, T. Espitau, S. Katsumata, M. Maller, F. Mouhartem, T. Prest, **M. Rossi**, Markku-Juhani Saarinen, « Raccoon. A Side-Channel Secure Signature Scheme ».
En savoir plus

Laboratoire de la sécurité des technologies sans-fil

T. Claverie, G. Avoine, S. Delaune, **J. Lopes Esteves**, « Tamarin-Based Analysis of Bluetooth Uncovers Two Practical Pairing Confusion Attacks », ESORICS 2023, Lecture Notes in Computer Science, The Hague, Netherlands, Springer, 2023.
En savoir plus

Laboratoire exploration et recherche en détection

C. Larroche, « A source separation approach to temporal graph modelling for computer networks », MLCS 2023 (ECML workshop).
En savoir plus

L. Aubard, **J. Mazel**, G. Guette, **P. Chifflier**, O. Levillain, G. Blanc, L. Mé, « Modélisation et test des ambiguïtés de recouvrement de données pour l'obtention des politiques de réassemblage dans les protocoles réseaux », Rendez-vous de la Recherche et de l'Enseignement de la Sécurité des Systèmes d'Information (RESSI), 2023.
En savoir plus

Laboratoire sécurité du logiciel

M. Baty, P. Wilke, G. Hiet, **A. Fontaine**, **A. Trieu**, « A Generic Framework to Develop and Verify Security Mechanisms at the Microarchitectural Level: Application to Control-Flow Integrity », 2023 IEEE 36th Computer Security Foundations Symposium (CSF), Dubrovnik, Croatia, 2023, pp. 372-387.
En savoir plus

Laboratoire sécurité réseau, protocole

V. Cortier, P. Gaudry, S. Glondu, **S. Ruhault**, « French 2022 legislatives elections: a verifiability experiment », E-Vote-ID 2023.
En savoir plus

A. Ebalard, R. Benadjila, « Randomness of random in Cisco ASA », SSTIC 2023.
En savoir plus

Laboratoire architecture matérielle et logicielle

V. Giraud, **G. Bouffard**, « Faulting original mceliece's implementations is possible: How to mitigate this risk? », Symposium on Security and Privacy, EuroS&P 2023 -Workshops on the Security of Software/Hardware Interfaces (SILM), pages 311–319.
En savoir plus

Laboratoire sécurité des composants

S. Boussam, J. Eynard, **G. Renault**, G. Zaïd, « Étude critique d'une méthode de Machine Learning appliquée à l'analyse par canaux auxiliaires », SSTIC 2023.
En savoir plus

Contributions à des ouvrages scientifiques

Laboratoire cryptologie

A. Dupin, P. Méaux, **M. Rossi**, « On the Algebraic Immunity – Resiliency trade-off, implications for Goldreich's Pseudorandom Generator », Journal DCC, 2023.
En savoir plus

H. Gilbert, J. Jean, « Differential Cryptanalysis », Chapitre dans l'Encyclopédie Sciences, Livre collectif Symmetric Cryptography, vol. 2, pp 3-26, ISTE Wiley 2023.
En savoir plus

Laboratoire sécurité des composants

F. Morain, **G. Renault**, B. Smith, « Deterministic factoring with oracles », article de journal dans Applicable Algebra in Engineering, Communication and Computing, Volume 34.
En savoir plus

R. Poussier, « Divide-and-Conquer Side-Channel Attacks », article Springer en ligne dans Encyclopedia of Cryptography, Security and Privacy.
En savoir plus

Laboratoire sécurité du logiciel

A.L. Georges, A. Guéneau, T. Van Strydonck, A. Timany, **A. Trieu**, D. Devriese, L. Birkedal, « Cerise: Program Verification on a Capability Machine in the Presence of Untrusted Code », article dans Journal of the ACM, 2023.
En savoir plus

Laboratoire exploration et recherche en détection

L. Masure, **R. Strullu**, « Side-channel analysis against ANSSI's protected AES implementation on ARM: end-to-end attacks with multi-task learning », article dans le Journal of Cryptographic Engineering, 2023.
En savoir plus

Laboratoire de la sécurité des technologies sans-fil

J. Lopes Esteves, P-M. Ricordel, and K. Redon, « Des Pare-Feux Pour Le HDMI », article dans le journal MISC n°127, May 2023.
En savoir plus

PUBLICATIONS OPEN SOURCE

Hackropole : site d'archivage du French CyberSecurity Challenge et mise en ligne du serveur Hackropole.
En savoir plus

Chipsec-check : outil de validation de conformité d'exigences matérielles.
Code source Github

DroidWorks : outil d'analyse d'APK (Android Package Kit).
Code source Github

Lidi : diode TCP unidirectionnelle.
Code source Github

Ultrablue : contrôle d'intégrité du démarrage d'un PC via Bluetooth.
Code source Github

Shovel : interface graphique permettant d'utiliser l'outil Suricata de manière plus facile et intuitive.
Code source Github

CONTRIBUTIONS À DES PROJETS OPEN SOURCE TIERS

Linux-hardened : configuration et patchs de durcissement du noyau Linux.
Code source Github

Keysas : station blanche de décontamination USB.
Code source Github

Tamarin : outil de vérification de protocoles cryptographiques.
Code source Github

NixOS : distribution Linux basée sur le gestionnaire de paquet Nix.
Code source Github

Bootstrap : feuilles de style CSS permettant de développer une interface utilisateur web gardant un rendu homogène entre navigateurs web.
Code source Github.

Suricata : outil d'analyse de flot réseau.
Code source Github

File : outil pour reconnaître le type d'un fichier à partir de sa signature.
Code source Github

Rainbow : instrumentation de Qemu pour simuler des fuites par canaux auxiliaires ou des injections de fautes.
Code source Github

PyPDM : pilotage des modules PDM d'Alphanov.
Code source Github

RAPPORTS SUR LES MENACES ET INCIDENTS

Panorama de la cybermenace 2022. 24 janvier 2023.
En savoir plus

Cyber Threat Overview 2022. 10 février 2023.
En savoir plus

Le Ransomware-As-A-Service Lockbit. **14 juin 2023.**
En savoir plus

État de la menace informatique contre les cabinets d'avocats. **27 juin 2023.**
En savoir plus

Grands évènements sportifs – évaluation de la menace 2023. **30 août 2023.**
En savoir plus

Démantèlement du Botnet Qakbot. **18 septembre 2023.**
En savoir plus

FIN12 : un groupe cybercriminel aux multiples rançongiciels. **18 septembre 2023.**
En savoir plus

Synthèse de la menace ciblant les collectivités territoriales. **23 octobre 2023.**
En savoir plus

Campagnes d'attaques du mode opératoire APT28 depuis 2021. **26 octobre 2023.**
En savoir plus

État de la menace ciblant le secteur des télécommunications. **18 décembre 2023.**
En savoir plus

ALERTES DE SÉCURITÉ

16 alertes publiées sur le site du CERT-FR en 2023.
En savoir plus

PARTENARIAT

Rapport annuel conjoint ANSSI-BSI sur la vérification d'identité à distance.
En savoir plus

RÉFÉRENTIEL

Référentiel d'exigences applicables aux prestataires d'accompagnement et de conseil en sécurité des systèmes d'information (PACS). Version 1.0 du 19 juillet 2023 (publié le 26 septembre 2023).
En savoir plus

Légende

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