UNIVERSITÉ PARIS CITÉ

NOVEMBRE 2022

Compte Rendu du Lundi de la Cybersécurité

Les attaques par canaux cachés

ORGANISATEURS

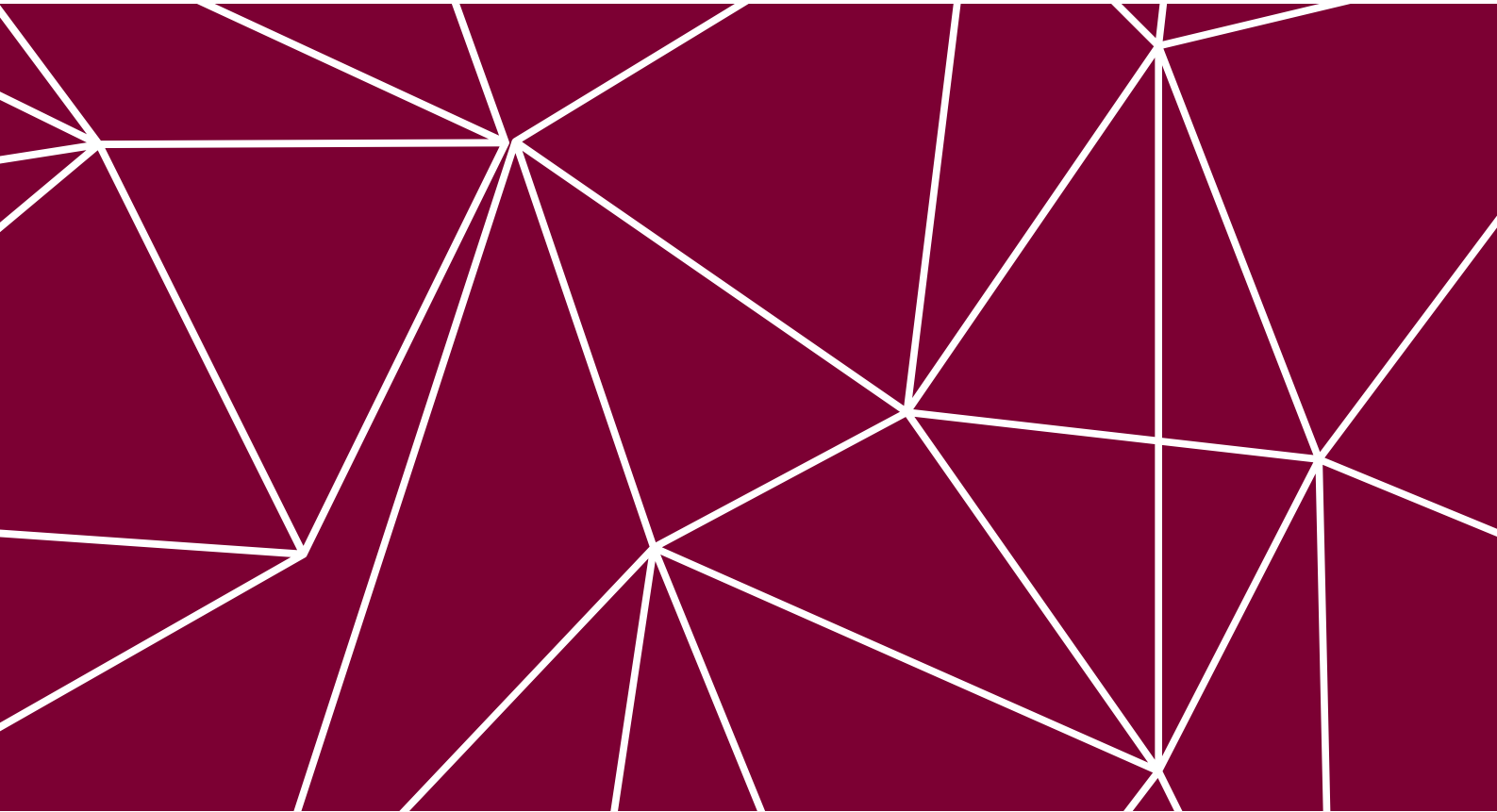
Gerard Peliks
Ahmed Mehaoua
Béatrice Laurent

INTERVENANTS

Jean Jacques Quisquater
David Samyde
Philippe Lavault

COMPTE RENDU

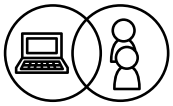
Imene Goucem
imene.goucem@etu.u-paris.fr



Université Paris Cité
45 Rue des Saints-Pères, Paris 6ème

lundi 14 novembre 2022

de 18h00 à 20h00



en hybride

320 inscrits

Les attaques par canaux cachés

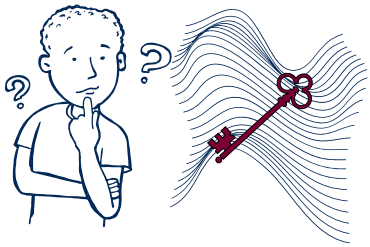
(ou canaux auxiliaires)

Jean-Jacques Quisquater

est un cryptologue belge figurant parmi les pionniers de la blockchain et de la carte à puce:

- Professeur à l'université catholique de Louvain en Belgique;
- Membre de l'ARCSI;
- Docteur d'État en science informatique obtenu au Laboratoire de recherche en informatique de l'université d'Orsay;
- Membre de l'IEEE;
- Académicien à l'Académie royale de Belgique.

Et si on pouvait accéder aux clés secrètes en écoutant les ondes électromagnétiques ?



→ Et bien, la réponse est: **OUI**

Effectivement, un calculateur qui déroule un algorithme cryptographique consomme du courant électrique, avec des pics et des creux qu'un oscilloscope révèle. Cela induit des vulnérabilités qui peuvent renseigner sur les clés de chiffrement.

Hormis la consommation électrique, d'autres moyens nous permettent d'accéder aux secrets, parmi:

- les signaux électromagnétiques qui se propagent, devenant alors susceptibles d'être interceptés et enregistrés pour être au cœur de beaucoup de calculs visant à révéler les secrets.
- Les changements de tension au sein d'une résistance ou d'un condensateur s'accompagnent de vibrations mécaniques qui peuvent être sujettes à des analyses très approfondies.
- L'activité électromagnétique, le bruit, le temps d'exécution d'un ordinateur qui opère une activité de chiffrement peuvent renseigner sur les clés de chiffrement utilisées.

Les attaques par canaux cachés

(ou canaux auxiliaires)

Certes, ce travail de cryptanalyse n'est évidemment pas à la portée de tous , mais avec le bon équipement, **c'est bien envisageable...**

Nous avons eu droit à trois démos avec le Professeur Jean-Jacques Quisquater, à savoir:

- Un thermomètre infrarouge
- Une caméra infrarouge
- Une mesure de consommation de pages web

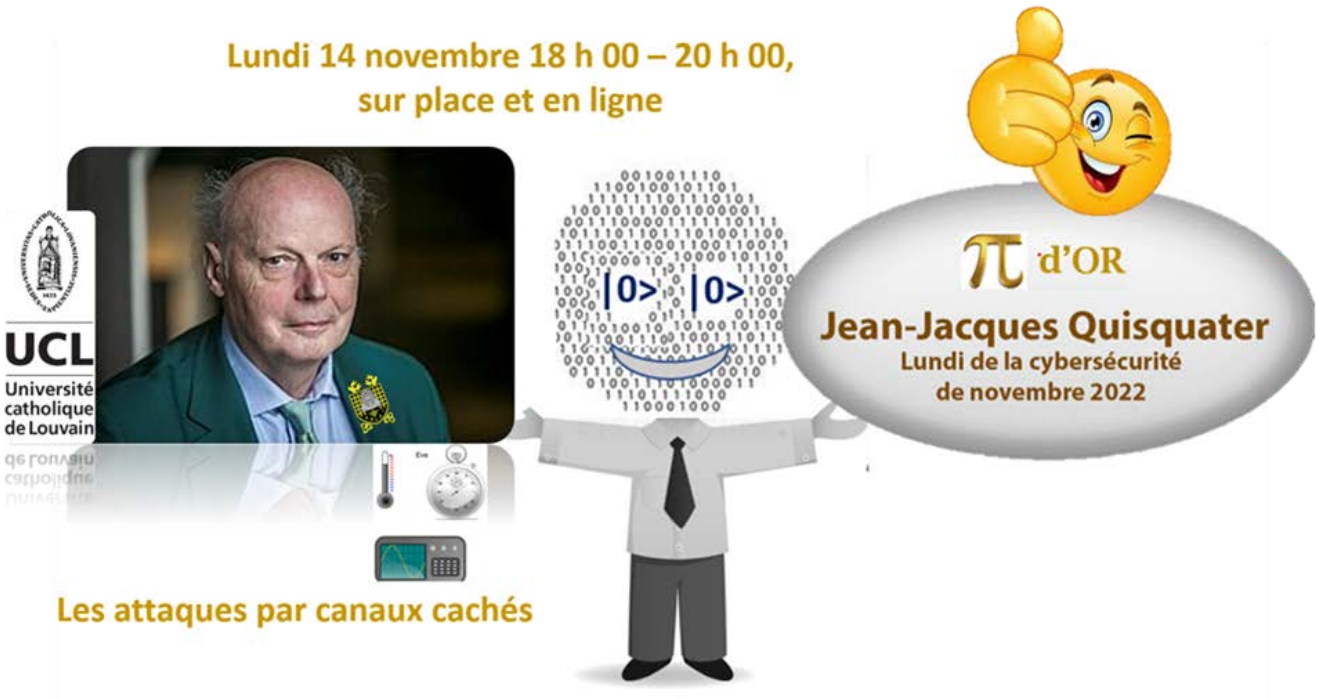
En somme,

Cette intervention nous alerte sur les attaques qui exploitent des canaux secondaires, peu communs, mais très redoutables, aussi appelés "canaux cachés" !
Alors, quelles que soient les mesures de sécurité que nous pouvons prendre, nos secrets ne sont pas si protégés que ça!

Au passage du 314e inscrit,
le Pr. Quisquater obtient

Le trophée du π d'or

des "Lundi de la Cybersécurité"



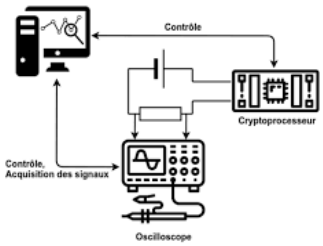
Application des attaques par canaux cachés aux microarchitectures

David Samyde

est:

- Ingénieur en électronique;
- Ingénieur en Sécurité;
- Panorama de réalisations analogiques et digitales;
- Une vingtaine d'années d'expérience en sécurité de Intel aux GAFAM, en passant par des entreprises du domaine bancaire.

Le spécialiste nous a expliqué les principales attaques par canaux auxiliaires sur différentes microarchitectures:



- leur genèse
- leurs avancées les plus récentes
- les risques afférents et leur impact réel compris dans le cloud

En conclusion,

Les attaques par canal auxiliaire sur la micro-architecture des processeurs font l'objet de multiples recherches. Auparavant peu connues du grand public, et concernant essentiellement les implémentations d'algorithmes cryptographiques, ces attaques ont pris le devant de la scène et se sont beaucoup développées ces dernières années avec les attaques Meltdown et Spectre.

Un quart d'heure avec l'ANSSI

Philippe Lavault

est

- chef des ressources extérieures de l'Agence nationale de la sécurité des systèmes d'information (ANSSI);
- Secrétaire général du club de réflexion de l'ANSSI;
- Conferencier à Sciences Po Lille;
- Co-auteur du thriller captivant : le protocole Magog.

Philippe Lavault nous a présenté l'Agence nationale de la Sécurité des Systèmes d'Information qui découle de l'intuition stratégique française par la décision du Général de Gaulle de séparer l'attaque et la défense en 1943. L'ANSSI est donc un organisme de **défense** chargé d'accompagner et de sécuriser le développement du numérique. Elle est désormais un acteur majeur de la cybersécurité en France.

L'intervenant a insisté sur le caractère défensif de l'ANSSI, et a ensuite développé le **rôle** de l'agence auprès des:

- Opérateurs d'Importance Vitale (OIV)
- Opérateurs de Services Essentiels (OSE)
- Ministères

En cas d'attaque soupçonnée ou avérée, un organe de l'ANSSI appelé le Centre Opérationnel de la Sécurité des Systèmes d'Information (COSSI) met en œuvre des dispositifs de veille, de collecte, de détection et d'analyse afin d'assurer la défense des services de l'état et des opérateurs les plus sensibles.

On se donne rendez-vous au...

Prochain lundi de la cybersécurité

le 05 décembre 2022

Qui portera sur:

"Les territoires de confiance numérique"

Avec

Bénédicte Pilliet

Présidente du Cybercercle