JAIF 2020v2

Jeudi 24 septembre 2020
ENS Paris / Grenoble, Minatec

Guillaume Bouffard, ENS/ANSSI
Damien Couroussé, CEA
Sylvain Guilley, Telecom ParisTech / Secure-IC
Karine Heydemann, Sorbonne Université / LIP6
Marie-Laure Potet, Univ. Grenoble Alpes / Vérimag

Remerciements

Soutien institutionnel:

- GDR Sécurité Informatique
- ENS
- Cybersecurity Institute
- CEA
- IRT NanoElec

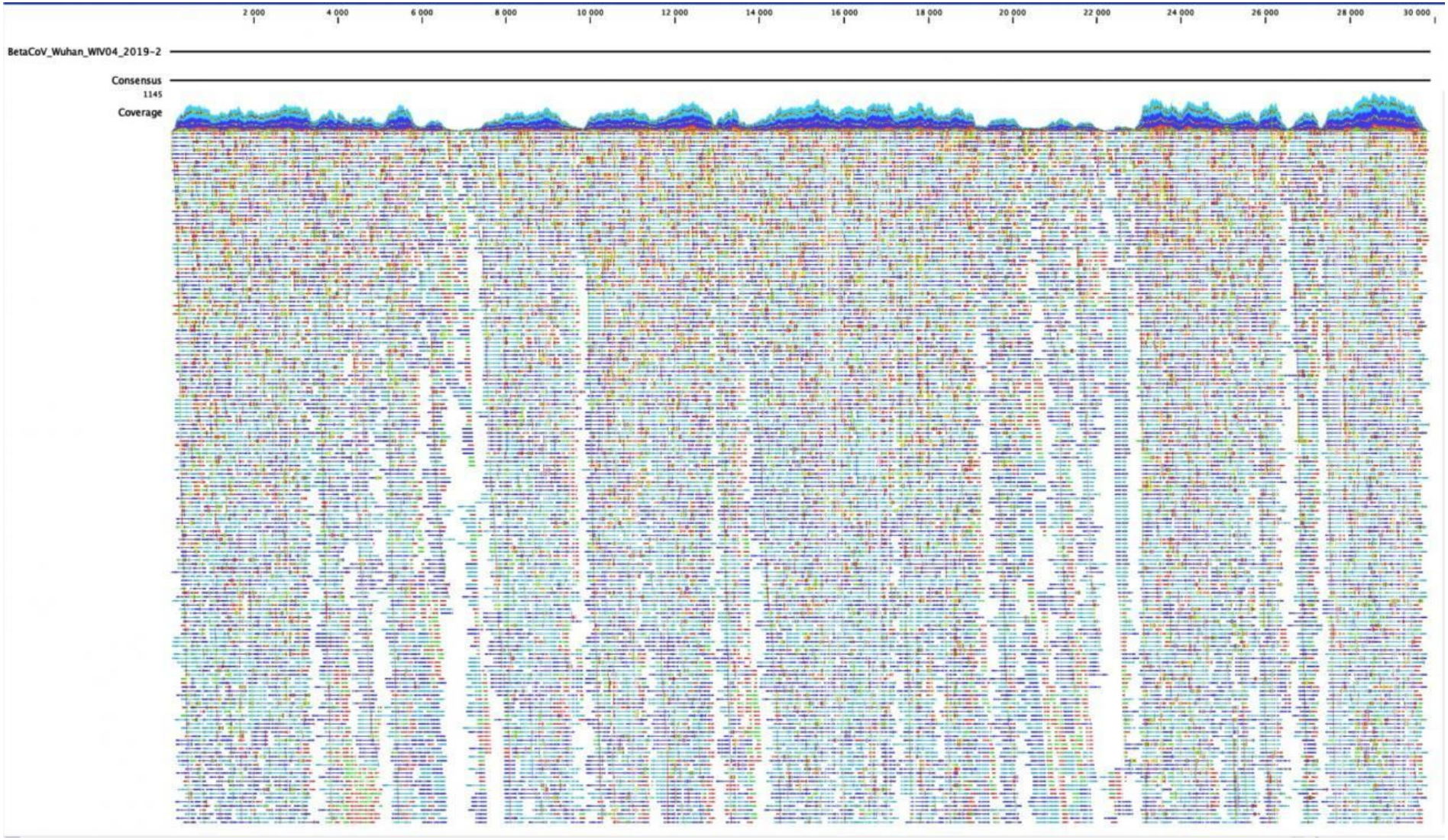
Sponsors:

- ARM
- IDEMIA
- INVIA
- Ledger
- Serma Safety & Security

Previously …

- JAIF 2020 est la 4e édition
- Journée intialement prévue le 18 mars 2020

Un invité surprise



À mesures exceptionnelles, organisation exceptionnelle

- Salles très limités en participants
- 3 moyens d'assister à JAIF 2020
  - Salle Dussane à l'ENS Ulm, Paris
  - Salle Palladium, Minatec, Grenoble
  - Sur Zoom
- Plus de participants attendus que dans la v1
  - 140 inscrits

Règles sanitaires à respecter

- Port du masque obligatoire
- Interdiction de groupe de plus de 10 personnes
- Gel hydroalcoolique et lingettes disponibles
- **Liste d'émargement à signer !**

Pauses

Pour Paris

- Pas de pause café autorisée 😞
  - *Mais vous pouvez utiliser la machine à café*
- Pas de déjeuner ensemble 😞
  - *Il y a assez de restaurants autour*

Pour Grenoble:

- Pause café et plateaux repas 😀

Programme – matinée

10:00-10:10 – Introduction à la journée

10:10-11:25 – Session #1. Injection de fautes

- **Discussion of the laser and EM Instruction Skip Fault Models**
  Jean-Max Dutertre (EMSE)
- **Keep it Cheap: Multiple Faults Attacks in Practice**
  Karim M. Abdellatif et Olivier Hériveaux (Ledger)
- **Méthodologie d'analyse de vulnérabilité en présence de faute multiple**
  Vincent Werner (CEA/LETI)
- **Questions et échanges**

11:25-11:35 – Pause

11:35-12:00 – Session #2. Questions ouvertes sur la sécurité des systèmes

- **A journey to Soft IP Common Criteria Certification**
  Christophe Evrard (ARM)
- **Questions et échanges**

12:00-13:30 – Déjeuner

Programme – après-midi

13:30-14:45 – Session #3. Protections logicielles

- **BISM: Bytecode-Level Instrumentation for Software Monitoring**
  Chukri Soueidi, Ali Kassem, and Ylies Falcone (INRIA)
- **Propagation et préservation de propriétés dans un flot de compilation optimisant et applications à la préservation de protections contre les attaques en faute**
  Son Tuan Vu (Sorbonne Université/LIP6)
- **Analyse et placement de contremesures logicielles contre l'injection de faute en multi-faute**
  Étienne Boespflug (Université Grenoble Alpes)
- **Questions et échanges**

14:45-15:00 – Pause

14:50-15:40 – Session #4. Architecture et exploitabilité

- **Bridging the Gap between RTL and Software Fault Injection: a Methodology for Accurate Fault Modeling**
  Johan Laurent (LCIS)
- **Perturbation attacks on modern CPU, from the fault model to the exploitation**
  Thomas Trouchkine (ANSSI)
- **Questions et échanges**

15:45 – Conclusion de la journée

Des questions ?