List of Papers

This is the list of papers to choose from. Send your top 3 preferences to the instructor and all efforts will be made to accommodate them.

1. Gilles Barthe, Sandrine Blazy, Benjamin Gregoire, Remi Hutin, Vincent Laporte, David Pichardie, Alix Trieu: Formal verification of a constant-time preserving C compiler. Proc. ACM Program. Lang. 4(POPL): 7:1-7:30 (2020)

2. Jose Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Arthur Blot, Benjamin Gregoire, Vincent Laporte, Tiago Oliveira, Hugo Pacheco, Benedikt Schmidt, Pierre-Yves Strub: Jasmin: High-Assurance and High-Speed Cryptography. ACM Conference on Computer and Communications Security 2017: 1807-1823

3. Gilles Barthe, Benjamin Gregoire, Vincent Laporte: Secure Compilation of Side-Channel Countermeasures: The Case of Cryptographic "Constant-Time". CSF 2018: 328-343

4. Michael Sammler, Deepak Garg, Derek Dreyer, Tadeusz Litak: The high-level benefits of low-level sandboxing. Proc. ACM Program. Lang. 4(POPL): 32:1-32:32 (2020)

5. Lau Skorstengaard, Dominique Devriese, Lars Birkedal: Reasoning about a Machine with Local Capabilities: Provably Safe Stack and Return Pointer Management. ACM Trans. Program. Lang. Syst. 42(1): 5:1-5:53 (2020)

6. Thomas Van Strydonck, Frank Piessens, Dominique Devriese: Linear capabilities for fully abstract compilation of separation-logic-verified code. Proc. ACM Program. Lang. 3(ICFP): 84:1-84:29 (2019)

7. Stelios Tsampas, Andreas Nuyts, Dominique Devriese, Frank Piessens: A categorical approach to secure compilation. CoRR abs/2004.03557 (2020)

8. Carmine Abate, Arthur Azevedo de Amorim, Roberto Blanco, Ana Nora Evans, Guglielmo Fachini, Catalin Hritcu, Theo Laurent, Benjamin C. Pierce, Marco Stronati, Andrew Tolmach: When Good Components Go Bad: Formally Secure Compilation Despite Dynamic Compromise. ACM Conference on Computer and Communications Security 2018: 1351-1368

9. Weird Machines as Insecure Compilation: Jennifer Paykin, Eric Mertens, Mark Tullsen, Luke Maurer, Benoit Razet, Alexander Bakst, Scott Moore. CoRR abs/1911.00157 (2020) (aka Exploits as Insecure Compilation)

10. Gabriel Scherer, Max S. New, Nick Rioux, Amal Ahmed: FabULous Interoperability for ML and a Linear Language. FoSSaCS 2018: 146-162