Monday

Time	Person/Lead	Topic	Duration
07:30-08:45	breakfast		
09:15-10:00	welcome, organization, and introductions		
10:00-10:30	coffee @ Cafeteria (S006 in the castle)		
10:30-12:15	Lead: Mathias Payer (remote)	Discussion: Real-world deployment (incl. bridging formal methods and practical deployment) + remaining frontiers for secure compilation research	
12:15-14:00	lunch		
14:00-14:30	Dominique Devriese	Formalizing ISA security guarantees in the form of universal contracts	30 mins
14:30-14:50	Jan Reineke	Hardware-Software Contracts and Secure Programming	20 mins
14:50-15:10	Marco Guarnieri	Hardware-Software Security Contracts and Secure Compilation	20 mins
15:10-15:40	Marco Patrignani	Compositional Secure Compilation against Spectre	30 mins
15:40-16:10	Gang Tan	Compiler-based side-channel detection and mitigation	30 mins, remote (EST)
16:10-16:40	cake		
16:40-17:10	Gilles Barthe	Enforcement and compiler preservation of fine-grained constant-time policies	30 mins, remote (CET)
17:10-17:40	Drew Zagieboylo	Verifying Speculation Security of Processor Implementations	30 mins, remote (EST)
17:40-18:00	Deian Stefan	Swivel: Hardening WebAssembly against Spectre	20 mins, remote (PST)

Tuesday

Time	Person/Lead	Topic	Duration
07:30-08:45	breakfast		
09:00-10:00		Spare time, for instance for working in small groups	
10:00-10:30	coffee @ Cafeteria (S006 in the castle)		
10:30-12:15	Lead: Marco Guarnieri	Discussion: Micro-architectural attacks and countermeasures + Secure compilation against side-channels	
12:15-14:00	lunch		
14:00-14:40	Peter Sewell	Morello status and verification	40 mins, remote (UK)
14:40-15:10	Shweta Shinde	A Wishlist for the Next Generation of Trusted Execution Environments	30 mins
15:10-15:40	Stefan Brunthaler	Are Compiler Optimizations Doing it Wrong? An Investigation of Array Bounds Checking Elimination	30 mins
15:40-16:00	David Chisnall	Project Verona: An abstract machine allowing partial verification	20 mins, remote (UK)
16:00-16:30	cake @ Restaurant		
16:30-17:00	Thomas Van Strydonck	Cerise: Program Verification on a Capability Machine in the Presence of Untrusted Code	30 mins
17:00-17:30	Mads Dam	On information flow preserving refinement	30 mins, remote (CET)
17:30-17:50	Kostya Serebryany	Hardware-assisted testing in production	20 mins, remote (PST)
17:50-18:00	Marco Patrignani	Compositional Secure Compilation against Spectre (continued)	10 mins
18:30-19:30	dinner		
19:30-21:00	Organizers: Mathias Payer and David Chisnall	All-hands social (on-site and remote) on Gathertown	

Wednesday

Time	Person/Lead	Topic	Duration
07:30-08:45	breakfast		
09:00-10:00		Spare time, for instance for working in small groups	
10:00-10:30	coffee @ Cafeteria (S006 in the castle)		
10:30-12:15	Lead: Shweta Shinde	Discussion: New security architectures (including TEEs, Morello, and verifying properties of such architectures).	
12:15-14:00	lunch		
14:00-14:40	Catalin Hritcu	Formally verifying a secure compilation chain for unsafe C components	40 mins
14:40-15:20	Akram El-Korashy	Proof techniques for secure compilation with memory sharing	40 mins
15:20-16:00	Chung-Kil Hur	Conditional Contextual Refinement	40 mins, remote (UK)
16:00-16:30	cake @ Restaurant		
16:30-17:00	Roberto Blanco	Formalizing Stack Safety as a Security Property	30 mins
17:00-17:40	Zhong Shao & Jérémie Koenig	CompCertO: Compiling Certified Open C Components	40 mins, remote (EST)
17:40-18:00	Ingrid Verbauwhede	How we design hardware and what it costs?	20 mins

Thursday

Time	Person/Lead	Topic	Duration
07:30-08:45	breakfast		
09:00-10:00	Lead: Catalin Hritcu	Short hike around Dagstuhl (starting at Cafeteria)	
10:00-10:30	coffee @ Cafeteria (S006 in the castle)		
10:30-12:15	Lead: Dominique Devriese	Discussion: Verification techniques (broad verification frameworks and specific proof techniques for secure compilation)	
12:15-13:40	lunch + photo		
13:40-14:00	Ingrid Verbauwhede	How we design hardware and what it costs? (continued)	20 mins
14:00-14:40	Mathias Payer	Automatic inference of effective compartmentalization policies	40 mins, remote (CET)
14:40-15:20	Nathan Burow	Cross-Language Attacks	40 mins, remote (EST)
15:20-15:50	Zoe Paraskevopoulou	WebAssembly as an intermediate language for safe interoperability	30 mins, remote (EST)

15:50-16:00	Matteo Busi	Securing Interruptible Enclaved Execution on Small Microprocessors	10 mins	
16:00-16:30	cake @ Restaurant			
16:30-17:10	Anitha Gollamudi	Preserving Memory Safety from C to MSWasm	40 mins	
17:10-17:40	Nikos Vasilakis	Software Supply Chains: Challenges and Opportunities	30 mins, remote (EST)	
17:40-18:00	Per Larsen	Changing Compilation without Changing the Compiler	20 mins, remote (PST)	

Friday

07:30-08:45	breakfast			
09:00-10:00	Lead: Deepak Garg	A wishlist of useful abstractions and try to see how they could apply to various kinds of targets		
10:00-10:30	coffee @ Cafeteria (S006 in the castle)			
10:30-12:15	Lead: David Chisnall (remote)	Discussion: Interoperability (interoperability between languages, varying trust between components, compartmentalization)		
12:15-14:00	lunch			