Syllabus

Date	Papers
Oct 1	**Overview and Introduction** How to Read a Paper by S. Keshav The Rise of Worse is Better by R. P. Gariel
	Low-Level Vulnerabilities and Defenses
Oct 3	How Memory Safety Violations Enable Exploitation of Programs by M. Payer A Modern History of Offensive Security Research by D. Dai Zovi *See also:* Low-Level Software Security by Example by U. Erlingssona et al.
Oct 8 [1]	Control-Flow Integrity: Precision, Security, and Performance by N. Burow et al. Control-Flow Bending: On the Effectiveness of Control-Flow Integrity by N. Carlini et al.
Oct 10	Principles and Implementation Techniques of Software-Based Fault Isolation by G. Tan Bringing the Web up to Speed with WebAssembly by A. Haas et al.
	Web Security
Oct 15 [2]	Beware of Finer-Grained Origins by C. Jackson and A. Barth Securing Frame Communication in Browsers by A. Barth et al. Chromium's design documents on Site Isolation and Cross-Origin Read Blocking The Web Origin Concept by A. Barth
Oct 17	Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers by M. T. Louw and V.N. Venkatakrishnan Robust Defenses for Cross-Site Request Forgery by A. Barth et al. Using positive tainting and syntax-aware evaluation to counter SQL injection attacks by W. G. J. Halfond et al.
Oct 22	CSP is dead, long live CSP! On the insecurity of whitelists and the future of content security policy by L. Weichselbaum et al. Protecting Users by Confining JavaScript with COWL by D. Stefan et al.
	Web Privacy
Oct 24	Who Left Open the Cookie Jar? A Comprehensive Evaluation of Third-Party Cookie Policies by G. Franken et al. An Analysis of Private Browsing Modes in Modern Browsers by G. Aggarwal et al. Browser History re:visited by M. Smith et al.
Oct 29	Trusted Browsers for Uncertain Times by D. Kohlbrenner and H. Shacham The Design and Implementation of the Tor Browser by M. Perry
	The Hardware-Software Boundary
Oct 31	Spectre Attacks: Exploiting Speculative Execution by P. Kocher et al. Meltdown: Reading Kernel Memory from User Space by M. Lipp et al. Foreshadow: Extracting the Keys to the Intel SGX Kingdom with Transient Out-of-Order Execution by J. Van Bulck et al.
Nov 5	Hyperflow: A Processor Architecture for Nonmalleable, Timing-Safe Information-Flow Security by A. Ferraiuolo et al. GhostRider: A Hardware-Software System for Memory Trace Oblivious Computation by C. Liu et al.
	Automatic Vulnerability Discovery
Nov 7	A Survey of Symbolic Execution Techniques by R. Baldoni et al. Under-Constrained Symbolic Execution: Correctness Checking for Real Code by D. A. Ramos and D. Engler SAGE: Whitebox Fuzzing for Security Testing by P. Godefroid et al.
Nov 19	AEG: Automatic Exploit Generation by T. Avgerinos et al. NAVEX: Precise and Scalable Exploit Generation for Dynamic Web Applications by A. Alhuzali et al. Driller: Augmenting Fuzzing Through Selective Symbolic Execution by N. Stephens et al.
	Package managers and sofware distribution
Nov 26	Docker ecosystem–Vulnerability Analysis by A. Martin et al. A Look In the Mirror: Attacks on Package Managers by J. Cappos et al.
Nov 28	CHAINIAC: Proactive Software-Update Transparency via Collectively Signed Skipchains and Verified Builds by K. Nikitin et al. Contour: A Practical System for Binary Transparency by M. Al-Bassam and S. Meiklejohn
	Stepping Back
Dec 3	Thirty Years Later: Lessons from the Multics Security Evaluation by P. A. Karger and R. R. Schell This World of Ours by J. Mickens Looking Back: Addendum by D. E. Bell
Dec 5	How to Write a Great Research Paper by S. P. Jones How to Give a Great Research Talk by S. P. Jones On Preparing Good Talks by R. Jhala

1. Form project groups.
2. Submit project proposal.