

Kevin Zhijie Chen

University of California, Berkeley
<http://www.cs.berkeley.edu/~kevinchn/>

☎ +1 510 545 2586
✉ kevinchn@cs.berkeley.edu

Education

- 2010–present **Graduate Student in Computer Science**, *University of California, Berkeley, U.S.*, Advisor: Prof. Dawn Song.
- 2006–2010 **BS in Computer Science**, *Peking University, China.*
- 2007–2010 **Dual Major in Mathematics**, *Peking University, China.*

Interests & Skills

- Research Topics Program analysis, bug finding, mobile security, malware, drive-by downloads, and system security in general
- Programming Skills As a programming language researcher, I really think it's the programming model that matters instead of a specific programming language, but if I have to list: C/C++, Java, OCaml, Python and Assembly.
- Other Web browser and its security issues, functional programming, virtualization, reverse engineering & vulnerability exploitation

Publication

- Aug. 2011 Chia Yuan Cho, Domagoj Babic, Pongsin Poosankam, **Kevin Zhijie Chen**, Edward XueJun Wu and Dawn Song, ***MACE: Model-inference-Assisted Concolic Exploration for Protocol and Vulnerability Discovery***, 20th USENIX Security Symposium, (USENIX Security'2011).
- May 2011 Noah Johnson, Juan Caballero, **Kevin Zhijie Chen**, Stephen McCamant, Pongsin Poosankam, Daniel Reynaud, Dawn Song, ***Differential Slicing: Identifying Causal Execution Differences for Security Applications***, 32nd IEEE Symposium on Security and Privacy, (Oakland'2011).
- Mar. 2011 **Kevin Zhijie Chen**, Guofei Gu, Jose Nazario, Xinhui Han, Jianwei Zhuge, ***Web-Patrol: Automated Collection and Replay of Web-based Malware Scenarios***, 6th ACM Symposium on Information, Computer and Communications Security, ASIACCS'2011).
- Dec. 2009 **Zhijie Chen**, Chengyu Song, Xinhui Han, Jianwei Zhuge, ***Detecting Heapspray in Drive-by Download Attacks Using Opcode Dynamic Instrumentation***, In Proceedings of The 2nd Conference on Vulnerability Analysis and Risk Assessment (VARA'2009).
- June 2009 Tengfei Lu, **Zhijie Chen**, Jianwei Zhuge, Xinhui Han, Wei Zou, ***Research and Implementation of Network Attack Flow Redirection Mechanism in the Honeyfarm Environment***, in Journal of Nanjing University of Posts and Telecommunications (Natural Science), 2009,29(3).
also in Proceedings of The 6th Chinese Information and Communication Security Conference (CCICS'2009) **Best Paper Award**

Experience

Ph.D student in Prof. Dawn Song's Group, UC Berkeley, 2010–present

DroidBlaze **Modelchecking Android applications:** We built a system for automatically extracting abstract models from applications through static analysis, and checking them against different security specifications.

Model-based testing of Android applications: We built a system to automatically infer a model for the application through dynamic analysis, and systematically test the application to achieve high coverage.

BitBlaze **Identifying causal execution differences for security applications:** I worked on program analysis topics, esp. binary program analysis for vulnerability discovery and malware analysis.

The Honeynet Project Full Member, <http://www.honey.net.org/>, 2009–present

Google Summer of Code, Google Inc. and The Honeynet Project, Summer, 2009

PHoneyC **Low-interaction honeyclients:** I'm one of the developers of PHoneyC, a virtual honeyclient for web-based malware detection, Mentor: Jose Nazario from the the Honeynet Project & Arbor Networks

Institute of Computer Science and Technology, Peking University, Beijing, China, 2008–2010

WebPatrol **Drive-by downloads analysis:** We built a large-scale detection and forensics system for web-based malware.

Icarus **Honeyfarm:** Icarus is a Honeyfarm prototype system for attack detection and malware collection. I was involved in the design of its architecture and developed the HI honeypot based on Argos(a HI honeypot using Dynamic Data Flow Analysis)

Graduate-level Courses

- CS262a *Advanced Topics in Computer System*, instructor: Prof. Eric Brewer
- CS294-28 *Internet/Network Security*, instructor: Prof. Vern Paxson
- EE219c *Computer-aided Verification*, instructor: Prof. Sanjit Seshia
- CS261 *Computer Security*, instructor: Prof. Dawn Song
- CS294-65 *Privacy Technologies: From Theory to Practice*, instructor: Prof. Dawn Song
- CS271 *Randomness and Computation*, instructor: Prof. Alistair Sinclair
- CS294-70 *Automated Bug Finding and Debugging*, instructor: Prof. Koushik Sen