Hao Chen

Email: hchencs@gmail.com haochen.org Phone: +1 415 625 3135

RESEARCH INTERESTS

AI-driven security and software engineering. Security of machine learning.

EDUCATION

University of California, Berkeley 1998-08 – 2004-06
PhD in Computer Science *Berkeley, CA, USA*

APPOINTMENTS

Department of Computer Science, University of California 2016-07 – present
Professor *Davis, CA, USA*

Department of Computer Science, University of California 2010-07 – 2016-06
Associate Professor *Davis, CA, USA*

Department of Computer Science, University of California 2004-07 – 2010-06
Assistant Professor *Davis, CA, USA*

HONORS AND AWARDS

- IEEE Fellow
- ACM Distinguished Member
- Outstanding Engineering Faculty Award, UC Davis, 2010
- CAREER Award, National Science Foundation, 2007

STUDENTS

- *Doctoral*: Liang Cai, Jiyu Chen, Jonathan Crussell, Benjamin Davis, Clint Gibler, Yifeng He, Francis Hsu, Gabriel Maganis, Yuan Niu, Yuyang Rong, Ryan Stevens, Matthew Van Gundy
- *Master*: Haitian Chen, Jeremy Erickson, Eric Gustafson, Kristen Kennedy, Denys Ma, Radmillo Racic, Jonathan Vronsky

SERVICES

Chair or co-chair of technical program committee

- IEEE Conference on Communications and Network Security (CNS) 2023
- IEEE Mobile Security Technologies (MoST) 2012, 2013

Editorial board

- Associate editor of ACM Transactions on Security and Privacy (TOPS), 2020–present

Member of program committee

- ACM Conference on Foundations of Data Science (FODS) 2020

- ACM Conference on Computer and Communications Security (CCS) 2017–2019, 2022, 2025
- IEEE Conference on Communications and Network Security (CNS) 2013–2017
- ACM Asia Conference on Computer and Communications Security (ASIACCS) 2006, 2016–2017
- IEEE Mobile Security Technologies (MoST) 2012–2017
- IEEE International Conference on Computer Communications (INFOCOM) 2016
- IEEE Symposium on Security and Privacy (S&P) 2009, 2015
- International Conference on Mobile Systems, Applications, and Services (MobiSys) 2015
- International Conference on Cryptology and Network Security (CANS) 2015
- Annual Computer Security Applications Conference (ACSAC) 2012–2013
- World Wide Web Conference (WWW) 2012
- ACM Conference on Wireless Network Security (WiSec) 2011, 2016
- Network and Distributed System Security Symposium (NDSS) 2006, 2008–2011
- International Conference on Security and Privacy in Communication Networks (SecureComm) 2007–2012
- IEEE Web 2.0 Security and Privacy (W2SP) 2009–2011, 2013
- International Conference on Distributed Computing Systems (ICDCS) 2008
- Usenix Security Symposium 2007

FUNDING

- UC Noyce Initiative, PI — 2023-10 – 2025-09
  AI for Cybersecurity — $1 000 000
- NSF 1956364, PI — 2020-07 – 2023-06
  SaTC: CORE: Small: Collaborative: Understanding and Detecting Memory Bugs in Rust — $199 997
- ARL CRA, PI — 2018-09 – 2020-12
  MACRO: Models for Enabling Continuous Reconfigurability of Secure Missions — $226 714
- NSF 1801751, PI — 2018-08 – 2023-07
  SaTC: CORE: Medium: Collaborative: Towards Robust Machine Learning Systems — $400 000
- Intel, PI — 2013-10 – 2017-09
  Science and Technology Center for Secure Computing (ISTC-SC) — $150 000
- UC Davis, co-PI — 2012-09 – 2015-08
  Research Investments in the Sciences and Engineering (RISE) — $860 000
- NSF 1018964, PI — 2010-08 – 2014-07
  Designing New Authentication Mechanisms using Hardware Capabilities in Advanced Mobile Devices — $500 000
- NSF 0831547, co-PI — 2008-11 – 2012-10
  Practical Privacy Preserving Technologies — $300 000

- University of California MICRO, PI — 2008-08 – 2009-12
  Leveraging Cellular Networks for Web Authentication — $11 250
- NSF 0644450, PI — 2007-07 – 2013-06
  CAREER: Securing Broadband Cellular Data Networks — $400 000
- AFOSR, PI — 2007-05 – 2012-04
  Helix: A Self-Regenerative Architecture for the Incorruptible Enterprise — $1 646 000
- I3P, PI — 2005-09 – 2007-08
  Institute for Information Infrastructure Protection Fellowship — $150 000
- NSF 0524826, PI — 2005-10 – 2006-09
  CT-ISG: Reasoning about Composable Intrusion Detection Systems — $179 110
- NSF 0520320, co-PI — 2005-09 – 2008-08
  NeTS-NBD: Automatic Validation, Optimization, and Adaptation of Distributed Firewalls for Network Performance and Security — $400 000
- Sprint, PI — 2007, 2008
  Gift — $60 000
- Microsoft, PI — 2007
  Gift — $5000
- Intel, co-PI — 2005
  Gift — $150 000

PUBLICATIONS

In journals

1. Rong, Y., Zhang, C., Liu, J. & **Chen**, **H.** Valkyrie: Improving Fuzzing Performance Through Deterministic Techniques. *Journal of Systems and Software* **209** (Mar. 2024).
2. Du, X., Chen, A., He, B., **Chen**, **H.**, Zhang, F. & Chen, Y. AflIot: Fuzzing on Linux-based IoT Device with Binary-Level Instrumentation. *Computers & Security* **122.** ISSN: 0167-4048 (2022).
3. Guo, Y., Li, Q., Zuo, W. & **Chen**, **H.** An Intermediate-level Attack Framework on The Basis of Linear Regression. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **45,** 2726–2735 (2022).
4. Liu, Y., Xu, Z., Fan, M., Hao, Y., Chen, K., **Chen**, **H.**, Cai, Y., Yang, Z. & Liu, T. ConcSpectre: Be Aware of Forthcoming Malware Hidden in Concurrent Programs. *IEEE Transactions on Reliability* **71,** 1174–1188 (2022).
5. Chen, J., Guo, Y., Zheng, Q. & **Chen**, **H.** Protect Privacy of Deep Classification Networks by Exploiting Their Generative Power. *Machine Learning* **110,** 651–674 (2021).
6. Han, W., Cao, C., **Chen**, **H.**, Li, D., Fang, Z., Xu, W. & Wang, X. senDroid: Auditing Sensor Access in Android System-Wide. *IEEE Transactions on Dependable and Secure Computing* **17,** 407–421 (2017).
7. Zhang, Y., Yang, M., Gu, G. & **Chen**, **H.** Rethinking Permission Enforcement Mechanism on Mobile Systems. *IEEE Transactions on Information Forensics & Security* **11,** 2227–2240 (2016).
8. Crussell, J., Gibler, C. & **Chen**, **H.** AnDarwin: Scalable Detection of Android Application Clones Based on Semantics. *IEEE Transactions on Mobile Computing* **14,** 2007–2019 (2015).
9. Van Gundy, M. & **Chen**, **H.** Noncespaces: Using Randomization to Defeat Cross-Site Scripting Attacks. *Computers & Security* **31,** 612–628 (2012).

10. Hsu, F., **Chen**, **H.** & Machiraju, S. WebCallerID: Leveraging Cellular Networks for Web Authentication. *Journal of Computer Security* **19,** 869–893 (2011).
11. Racic, R., Ma, D., **Chen**, **H.** & Liu, X. Exploiting and Defending Opportunistic Scheduling in Cellular Data Networks. *IEEE Transactions on Mobile Computing* **9,** 609–620. ISSN: 1536-1233 (2009).
12. Misherghi, G., Yuan, L., Su, Z., Chuah, C.-N. & **Chen**, **H.** A General Framework for Benchmarking Firewall Optimization Techniques. *IEEE Transactions on Network and Service Management* **5,** 227–238 (2008).
13. **Chen**, **H.**, Hu, J. & Sproat, R. Integrating Geometrical and Linguistic Analysis for E-mail Signature Block Parsing. *ACM Transactions on Information Systems* **17,** 343–366 (1999).

In conference proceedings

1. Rong, Y., Yu, Z., Weng, Z., Neuendorffer, S. & **Chen**, **H.** *IRFuzzer: Specialized Fuzzing for LLVM Backend Code Generation* in *IEEE/ACM International Conference on Software Engineering (ICSE)* (Ottawa, Ontario, Canada, Apr. 27–May 3, 2025).
2. Li, Q., Guo, Y., Zuo, W. & **Chen**, **H.** *Improved Generation of Adversarial Examples Against Safety-aligned LLMs* in *Neural Information Processing Systems (NeurIPS)* (Vancouver, Canada, Dec. 9–15, 2024).
3. Huang, J., Zhao, J., Rong, Y., Guo, Y., He, Y. & **Chen**, **H.** *Code Representation Pre-training with Complements from Program Executions* in *Conference on Empirical Methods in Natural Language Processing (EMNLP)* (Miami, Florida, USA, Nov. 12–16, 2024).
4. Xiong, W., Guo, Y. & **Chen**, **H.** *The Program Testing Ability of Large Language Models for Code* in *Conference on Empirical Methods in Natural Language Processing (EMNLP)* (Miami, Florida, USA, Nov. 12–16, 2024).
5. Lyu, Y., Xie, Y., Chen, P. & **Chen**, **H.** *Prompt Fuzzing for Fuzz Driver Generation* in *ACM Conference on Computer and Communications Security (CCS)* (Salt Lake City, UT, USA, Oct. 14–18, 2024).
6. He, Y., Huang, J., Rong, Y., Guo, Y., Wang, E. & **Chen**, **H.** *UniTSyn: A Large-Scale Dataset Capable of Enhancing the Prowess of Large Language Models for Program Testing* in *International Symposium on Software Testing and Analysis (ISSTA)* (Vienna, Austria, Sept. 16–20, 2024).
7. Lin, J., Guo, Y. & **Chen**, **H.** *Intrusion Detection at Scale with the Assistance of a Command-line Language Model* in *Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)* (Brisbane, Australia, June 24–27, 2024).
8. Li, Q., Guo, Y., Zuo, W. & **Chen**, **H.** *Improving Adversarial Transferability via Intermediate-level Perturbation Decay* in *Neural Information Processing Systems (NeurIPS)* (New Orleans, LA, USA, Dec. 10–16, 2023).
9. Li, Q., Guo, Y., Zuo, W. & **Chen**, **H.** *Towards Evaluating Transfer-based Attacks Systematically, Practically, and Fairly* in *Neural Information Processing Systems (NeurIPS)* (New Orleans, LA, USA, Dec. 10–16, 2023).
10. Chen, P., Xie, Y., Lyu, Y., Wang, Y. & **Chen**, **H.** *HOPPER: Interpretative Fuzzing for Libraries* in *ACM Conference on Computer and Communications Security (CCS)* (Copenhagen, Denmark, Nov. 26–30, 2023).
11. Lin, F., Bai, B., Guo, Y., **Chen**, **H.**, Ren, Y. & Xu, Z. *MHCN: a Hyperbolic Neural Network Model for Multi-view Hierarchical Clustering* in *International Conference on Computer Vision (ICCV)* (Paris, France, Oct. 4–6, 2023).
12. Zhao, J., Rong, Y., Guo, Y., He, Y. & **Chen**, **H.** *Understanding Programs by Exploiting (Fuzzing) Test Cases* in *Findings of the Association for Computational Linguistics (ACL)* (Toronto, Canada, July 9–14, 2023).

13. Li, Q., Guo, Y., Zuo, W. & **Chen**, **H.** *Making Substitute Models More Bayesian Can Enhance Transferability of Adversarial Examples* in *International Conference on Learning Representations (ICLR)* (Kigali, Rwanda, May 1–5, 2023).
14. Li, Q., Guo, Y., Zuo, W. & **Chen**, **H.** *Squeeze Training for Adversarial Robustness* in *International Conference on Learning Representations (ICLR)* (Kigali, Rwanda, May 1–5, 2023).
15. Rong, Y., Zhang, C., Liu, J. & **Chen**, **H.** *Valkyrie: Improving Fuzzing Performance Through Deterministic Techniques* in *IEEE International Conference on Software Quality, Reliability, and Security (QRS)* (Guangzhou, China, Dec. 5–9, 2022). Best paper award.
16. Chen, J., Guo, Y., **Chen**, **H.** & Gong, N. *Membership Inference Attack in Face of Data Transformations* in *IEEE Conference on Communications and Network Security (CNS)* (Austin, TX, USA, Oct. 3–5, 2022).
17. Liu, B., Bai, B., Xie, W., Guo, Y. & **Chen**, **H.** *Task-optimized User Clustering based on Mobile App Usage for Cold-start Recommendations* in *ACM SIGKDD Conference on Knowledge Discovery and Data Mining* (Washington DC, USA, Aug. 14–18, 2022).
18. Jiang, Y., Cao, X., **Chen**, **H.** & Gong, N. *Feder: communication-efficient byzantine-robust federated learning* in *ICLR Workshop on Socially Responsible Machine Learning (SRML)* (Apr. 29–29, 2022).
19. Liu, Y., Fan, M., Liu, T., Hao, Y., Xu, Z., Chen, K., **Chen**, **H.** & Cai, Y. *ConcSpectre: Be Aware of Forthcoming Malware Hidden in Concurrent Programs* in *IEEE International Conference on Software Quality, Reliability, and Security (QRS)* (Dec. 6–10, 2021). Best paper award.
20. Liu, Z., Zhu, S., Qin, B., **Chen**, **H.** & Song, L. *Automatically Detecting and Fixing Concurrency Bugs in Go Software Systems* in *International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS)* (Apr. 19–23, 2021).
21. Guo, Y., Li, Q. & **Chen**, **H.** *Backpropagating Linearly Improves Transferability of Adversarial Examples* in *Neural Information Processing Systems (NeurIPS)* (Dec. 6–12, 2020).
22. Li, Q., Guo, Y. & **Chen**, **H.** *Practical No-box Adversarial Attacks against DNNs* in *Neural Information Processing Systems (NeurIPS)* (Dec. 6–12, 2020).
23. Chen, H., Jiang, B. & **Chen**, **H.** *StyleCAPTCHA: CAPTCHA Based on Style-Transferred Images to Defend against Deep Convolutional Networks* in *ACM-IMS Foundations of Data Science Conference (FODS)* (Oct. 18–20, 2020).
24. Rong, Y., Chen, P. & **Chen**, **H.** *Integrity: Finding Integer Errors by Targeted Fuzzing* in *International Conference on Security and Privacy in Communication Networks (SecureComm)* (Oct. 21–23, 2020).
25. Li, Q., Guo, Y. & **Chen**, **H.** *Yet Another Intermediate-Level Attack* in *European Conference on Computer Vision (ECCV)* (Aug. 23–28, 2020).
26. Jia, Y., Lu, Y., Shen, J., Chen, Q. A., **Chen**, **H.**, Zhong, Z. & Wei, T. *Fooling Detection Alone Is Not Enough: Adversarial Attack Against Multiple Object Tracking* in *International Conference on Learning Representations (ICLR)* (Addis Ababa, Ethiopia, Apr. 26–30, 2020).
27. Chen, J., Wang, D. & **Chen**, **H.** *Explore the Transformation Space for Adversarial Images* in *ACM Conference on Data and Application Security and Privacy (CODASPY)* (New Orleans, LA, USA, Mar. 16–18, 2020).
28. Chen, J., Huang, H. & **Chen**, **H.** *Informer: Irregular Traffic Detection for Containerized Microservices RPC in the Real World* in *ACM/IEEE Workshop on Security and Privacy in Edge Computing (Edge S&P)* (Washington DC, USA, Nov. 7–9, 2019).
29. Chen, P., Liu, J. & **Chen**, **H.** *Matryoshka: Fuzzing Deeply Nested Branches* in *ACM Conference on Computer and Communications Security (CCS)* (London, UK, Nov. 11–15, 2019).
30. Yen, C.-C., Ghosal, D., Zhang, M., Chuah, C.-N. & **Chen**, **H.** *Falsified Data Attack on Backpressure-Based Traffic Signal Control Algorithms* in *IEEE Vehicular Networking Conference (VNC)* (Taipei, Taiwan, Dec. 5–7, 2018).

31. Liu, Y., Chen, J. & **Chen**, **H.** *Less Is More: Culling the Training Set to Improve Robustness of Deep Neural Networks* in *Conference on Decision and Game Theory for Security (GameSec)* (Seattle, WA, USA, Oct. 29–31, 2018).
32. Chen, P. & **Chen**, **H.** *Angora: Efficient Fuzzing by Principled Search* in *IEEE Symposium on Security & Privacy* (San Francisco, CA, USA, May 21–23, 2018).
33. Zhang, Y., Dai, J., Zhang, X., Huang, S., Yang, Z., Yang, M. & **Chen**, **H.** *Detecting Third-Party Libraries in Android Applications with High Precision and Recall* in *IEEE International Conference on Software Analysis, Evolution, and Reengineering (SANER)* (Campobasso, Italy, Mar. 20–23, 2018).
34. Meng, D. & **Chen**, **H.** *MagNet: a Two-Pronged Defense Against Adversarial Examples* in *ACM Conference on Computer and Communications Security (CCS)* (Dallas, TX, Oct. 30–Nov. 3, 2017).
35. Wu, Y., Meng, D. & **Chen**, **H.** *Evaluating Private Modes in Desktop and Mobile Browsers and Their Resistance to Fingerprinting* in *IEEE Conference on Communications and Network Security (CNS)* (Las Vegas, NV, Oct. 9–11, 2017).
36. Vronsky, J., Stevens, R. & **Chen**, **H.** *SurgeScan: Enforcing Security Policies on Untrusted Third-Party Android Libraries* in *IEEE Conference on Advanced and Trusted Computing (ATC)* (San Francisco, CA, Aug. 4–8, 2017).
37. Chen, P. & **Chen**, **H.** *Security Analysis of Personal Unmanned Aerial Vehicles* in *International Conference on Security and Privacy in Communication Networks (SECURECOMM)* (Guangzhou, China, Oct. 10–12, 2016).
38. Qu, Z., Guo, G., Shao, Z., Rastogi, V., Chen, Y., **Chen**, **H.** & Hong, W. *AppShield: Enabling Multi-Entity Access Control Cross Platforms for Mobile App Management* in *International Conference on Security and Privacy in Communication Networks (SECURECOMM)* (Guangzhou, China, Oct. 10–12, 2016).
39. Fang, Z., Han, W., Li, D., Guo, Z., Guo, D., Wang, X. S., Qian, Z. & **Chen**, **H.** *RevDroid: Code Analysis of the Side Effects After Dynamic Permission Revocation of Android Apps* in *ACM Asia Conference on Computer and Communications Security (ASIACCS)* (Xi'an, China, May 30–June 3, 2016).
40. Stevens, R., Crussell, J. & **Chen**, **H.** *On the Origin of Mobile Apps: Network Provenance for Android Applications* in *ACM Conference on Data and Application Security and Privacy (CODASPY)* (New Orleans, LA, Mar. 9–11, 2016).
41. Stevens, R. & **Chen**, **H.** *Predictive Eviction: a Novel Policy for Optimizing TLS Session Cache Performance* in *IEEE Global Communications Conference: Communications and Information System Security (GLOBECOM)* (San Diego, CA, Dec. 6–10, 2015).
42. Zhang, Y., Yang, M., Gu, G. & **Chen**, **H.** *FineDroid: Enforcing Permissions with System-Wide Application* in *International Conference on Security and Privacy in Communication Networks (SECURECOMM)* (Dallas, TX, Oct. 26–29, 2015).
43. Cai, F., **Chen**, **H.**, Wu, Y. & Zhang, Y. *AppCracker: Widespread Vulnerabilities in User and Session Authentication in Mobile Apps* in *IEEE Mobile Security Technologies (MoST)* (San Jose, CA, May 21, 2015).
44. Crussell, J., Stevens, R. & **Chen**, **H.** *MAdFraud: Investigating Ad Fraud in Android Applications* in *International Conference on Mobile Systems, Applications and Services (MobiSys)* (Bretton Woods, NH, USA, June 16–19, 2014).
45. Defreez, D., Shastry, B., **Chen**, **H.** & Seifert, J.-P. *A First Look At Firefox OS Security* in *IEEE Mobile Security Technologies (MoST)* (San Jose, CA, May 17, 2014).
46. Posnett, D., Kavaler, D., Gibler, C., **Chen**, **H.**, Devanbu, P. & Filkov, V. *Using and Asking: APIs Used in the Android Market and Asked About in stackoverflow* in *International Conference on Social Informatics (SocInfo)* (Kyoto, Japan, Nov. 25–27, 2013).

47. Crussell, J., Gibler, C. & **Chen**, **H.** *Scalable Semantics-Based Detection of Similar Android Applications* in *European Symposium on Research in Computer Security (ESORICS)* (Egham, U.K., Sept. 9–13, 2013).
48. Davis, B. & **Chen**, **H.** *Retrofitting Android Apps* in *International Conference on Mobile Systems, Applications and Services (MobiSys)* (Taipei, Taiwan, June 25–28, 2013).
49. Gibler, C., Stevens, R., Crussell, J., **Chen**, **H.**, Zang, H. & Choi, H. *Characterizing Android Application Plagiarism and Its Impact on Developers* in *International Conference on Mobile Systems, Applications and Services (MobiSys)* (Taipei, Taiwan, June 25–28, 2013).
50. Gustafson, E., Kennedy, K. & **Chen**, **H.** *Quantifying the Effects of Removing Permissions from Android Applications* in *IEEE Mobile Security Technologies (MoST)* (San Francisco, CA, May 23, 2013).
51. Stevens, R., Ganz, J., Devanbu, P., **Chen**, **H.** & Filkov, V. *Asking for (and About) Permissions Used by Android Apps* in *Working Conference on Mining Software Repositories (MSR)* (San Francisco, CA, May 18–19, 2013).
52. Crussell, J., Gibler, C. & **Chen**, **H.** *Attack of the Clones: Detecting Cloned Applications on Android Markets* in *European Symposium on Research in Computer Security (ESORICS)* (Pisa, Italy, Sept. 10–12, 2012).
53. Cai, L. & **Chen**, **H.** *On the Practicality of Motion Based Keystroke Infernce Attack* in *International Conference on Trust & Trustworthy Computing (TRUST)* (Vienna, Austria, June 13–15, 2012).
54. Gibler, C., Crussell, J., Erickson, J. & **Chen**, **H.** *AndroidLeaks: Automatically Detecting Potential Privacy Leaks in Android Applications on a Large Scale* in *International Conference on Trust & Trustworthy Computing (TRUST)* (Vienna, Austria, June 13–15, 2012).
55. Maganis, G., Shi, E., **Chen**, **H.** & Song, D. *Opaak: Using Mobile Phones to Limit Anonymous Identities Online* in *International Conference on Mobile Systems, Applications and Services (MobiSys)* (Low Wood Bay, Lake District, United Kingdom, June 26–28, 2012).
56. Davis, B., **Chen**, **H.** & Franklin, M. *Privacy-Preserving Alibi Systems* in *ACM Symposium on Information, Computer and Communications Security (ASIACCS)* (Seoul, South Korea, May 1–3, 2012).
57. Davis, B., Sanders, B., Khodaverdian, A. & **Chen**, **H.** *I-ARM-Droid: a Rewriting Framework for In-App Reference Monitors for Android Applications* in *IEEE Mobile Security Technologies (MoST)* (San Francisco, CA, May 24, 2012).
58. Stevens, R., Gibler, C., Crussell, J., Erickson, J. & **Chen**, **H.** *Investigating User Privacy in Android Ad Libraries* in *IEEE Mobile Security Technologies (MoST)* (San Francisco, CA, May 24, 2012).
59. Cai, L. & **Chen**, **H.** *TouchLogger: Inferring Keystrokes on Touch Screen from Smartph One Motion* in *6th USENIX Workshop on Hot Topics in Security (HotSec 11)* (San Francisco, CA, Aug. 9–9, 2011).
60. Niu, Y. & **Chen**, **H.** *Gesture Authentication with Touch Input for Mobile Devices* in *3rd International Conference on Security and Privacy in Mobile Information and Communication Systems (MobiSec)* (Aalborg, Denmark, May 17–19, 2011).
61. Cai, L., Zeng, K., **Chen**, **H.** & Mohapatra, P. *Good Neighbor: Ad Hoc Pairing of Nearby Wireless Devices by Multiple Antennas* in *Annual Network and Distributed System Security Symposium (NDSS)* (San Diego, CA, Feb. 6–9, 2011).
62. Davis, B. & **Chen**, **H.** *DBTaint: Cross-Application Information Flow Tracking Via Databases* in *USENIX Conference on Web Application* (Boston, MA, June 23–24, 2010).
63. Cai, L., Machiraju, S. & **Chen**, **H.** *CapAuth: a Capability-Based Handover Scheme* in *IEEE Conference on Computer Communications (INFOCOM)* (San Diego, CA, Mar. 15–19, 2010).
64. Goldberg, I., Ustaoglu, B., Van Gundy, M. & **Chen**, **H.** *Multi-Party Off-the-Record Messaging* in *ACM Conference on Computer and Communications Security (CCS)* (Chicago, IL, Nov. 9–13, 2009).

65. Hsu, F. & **Chen**, **H.** *Secure File System Services for Web 2.0 Applications* in *ACM Cloud Computing Security Workshop (CCSW 2009)* (Chicago, IL, Nov. 13–13, 2009).
66. Cai, L., Maganis, G., Zang, H. & **Chen**, **H.** *Mitigating DoS Attacks on the Paging Channel by Efficient Encoding in Page Messages* in *International Conference on Security and Privacy in Communication Networks (SecureComm)* (Athens, Greece, Sept. 14–18, 2009).
67. Cai, L., Machiraju, S. & **Chen**, **H.** *Defending Against Sensor-Sniffing Attacks on Mobile Phones* in *The First ACM SIGCOMM Workshop on Networking, Systems, Applications on Mobile Handhelds (MobiHeld)* (Barcelona, Spain, Aug. 17–17, 2009).
68. Ye, S., Wu, F., Pandey, R. & **Chen**, **H.** *Noise Injection for Search Privacy Protection* in *IEEE International Conference on Privacy, Security, Risk and Trust (PASSAT)* (Vancouver, Canada, Aug. 29–31, 2009).
69. Becker, J. & **Chen**, **H.** *Measuring Privacy Risk in Online Social Networks* in *Web 2.0 Security and Privacy (W2SP)* (Oakland, CA, May 21–21, 2009).
70. Van Gundy, M. & **Chen**, **H.** *Noncespaces: Using Randomization to Enforce Information Flow Tracking and Thwart Cross-Site Scripting Attacks* in *Annual Network and Distributed System Security Symposium (NDSS)* (San Diego, CA, Feb. 8–11, 2009).
71. Crites, S., Hsu, F. & **Chen**, **H.** *OMash: Enabling Secure Web Mashups Via Object Abstractions* in *ACM Conference on Computer and Communications Security (CCS)* (Alexandria, VA, Oct. 27–31, 2008), 99–107.
72. Niu, Y., Hsu, F. & **Chen**, **H.** *iPhish: Phishing Vulnerabilities on Consumer Electronics* in *Usability, Psychology, and Security 2008* (San Francisco, CA, Apr. 14–14, 2008).
73. Machiraju, S., **Chen**, **H.** & Bolot, J. *Distributed Authentication for Low-Cost Wireless Networks* in *Workshop on Mobile Computing Systems and Applications (HotMobile)* (Napa Valley, CA, Feb. 25–26, 2008), 55–59.
74. Racic, R., Ma, D., **Chen**, **H.** & Liu, X. *Exploiting Opportunistic Scheduling in Cellular Data Networks* in *Annual Network and Distributed System Security Symposium (NDSS)* (San Diego, CA, Feb. 10–13, 2008), 333–345.
75. Van Gundy, M., **Chen**, **H.**, Su, Z. & Vigna, G. *Feature Omission Vulnerabilities: Thwarting Signature Generation for Polymorphic Worms* in *Annual Computer Security Applications Conference (ACSAC)* (Miami Beach, FL, Dec. 10–14, 2007), 74–83.
76. Wang, Y.-M., Ma, M., Niu, Y. & **Chen**, **H.** *Spam Double-Funnel: Connecting Web Spammers with Advertisers* in *International World Wide Web Conference (WWW)* (Banff, Canada, May 8–12, 2007).
77. Niu, Y., Wang, Y.-M., **Chen**, **H.**, Ma, M. & Hsu, F. *A Quantitative Study of Forum Spamming Using Context-Based Analysis* in *Annual Network and Distributed System Security Symposium (NDSS)* (San Diego, CA, Feb. 28–Mar. 2, 2007), 79–92.
78. Hsu, F., **Chen**, **H.**, Ristenpart, T., Li, J. & Su, Z. *Back to the Future: a Framework for Automatic Malware Removal and System Repair* in *Annual Computer Security Applications Conference (ACSAC)* (Miami Beach, FL, Dec. 11–15, 2006).
79. Racic, R., Ma, D. & **Chen**, **H.** *Exploiting MMS Vulnerabilities to Stealthily Exhaust Mobile Phone's Battery* in *nternational Conference on Security and Privacy in Communication Network (SecureComm)* (Baltimore, MD, Aug. 28–Sept. 1, 2006).
80. Yuan, L., **Chen**, **H.**, Mai, J., Chuah, C.-N., Su, Z. & Mohapatra, P. *FIREMAN: a Toolkit for FIREwall Modeling and ANalysis* in *IEEE Symposium on Security and Privacy* (Berkeley, CA, May 21–24, 2006), 199–213.
81. Schwarz, B., **Chen**, **H.**, Morrison, D. W., Geoff, West, J., Lin, J. & Tu, W. *Model Checking an Entire Linux Distribution for Security Violations* in *Annual Computer Security Applications Conference (ACSAC)* (Tucson, Arizona, Dec. 5–9, 2005).

82. **Chen**, **H.** & Shapiro, J. *Using Build-Integrated Static Checking to Preserve Correctness Invariants* in *ACM Conference on Computer and Communications Security (CCS)* (Washington, DC, Nov. 25–29, 2004), 288–297.
83. **Chen**, **H.**, Dean, D. & Wagner, D. *Model Checking One Million Lines of C Code* in *Annual Network and Distributed System Security Symposium (NDSS)* (San Diego, CA, Feb. 4–6, 2004), 171–185.
84. **Chen**, **H.** & Wagner, D. *MOPS: an Infrastructure for Examining Security Properties of Software* in *ACM Conference on Computer and Communications Security (CCS)* (Washington, DC, Nov. 18–22, 2002), 235–244.
85. **Chen**, **H.**, Wagner, D. & Dean, D. *Setuid Demystified* in *USENIX Security Symposium* (San Francisco, CA, Aug. 5–9, 2002), 171–190.
86. Dumais, S., Cutrell, E. & **Chen**, **H.** *Optimizing Search by Showing Results in Context* in *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)* (Seattle, WA, Mar. 31–Apr. 5, 2001), 277–284.
87. Dumais, S., Cutrell, E. & **Chen**, **H.** *Classified Displays of Web Search Results* in *ASIST SIG/CR Classification Research Workshop* (Nov. 12, 2000), 87–90.
88. Dumais, S. & **Chen**, **H.** *Hierarchical Classification of Web Content* in *ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR)* (Athens, Greece, July 24–28, 2000), 256–263.
89. **Chen**, **H.** & Dumais, S. *Bringing Order to the Web: Automatically Categorizing Search Results* in *ACM SIGCHI Conference on Human Factors in Computing Systems (CHI)* (The Hague, The Netherlands, Apr. 1–6, 2000), 145–152.
90. **Chen**, **H.** & Ho, T. K. *Evaluation of Decision Forests on Text Categorization* in *SPIE Conference on Document Recognition and Retrieval VII* **3967** (San Jose, CA, Jan. 26–27, 2000), 191–199.
91. Sproat, R., Hu, J. & **Chen**, **H.** *Emu: an E-mail Preprocessor for Text-to-speech* in *Workshop on Multimedia Signal Processing* (Redondo Beach, CA, Dec. 7–9, 1998), 239–244.
92. **Chen**, **H.**, Hu, J. & Sproat, R. *E-mail Signature Block Analysis* in *International Conference on Pattern Recognition (ICPR)* (Brisbane, Australia, Aug. 16–20, 1998), 1153–1156.
93. **Chen**, **H.**, Agazzi, O. E. & Suen, C. Y. *Piecewise Linear Modulation Model of Handwriting* in *International Conference on Document Analysis and Recognition (ICDAR)* (Ulm, Germany, Aug. 18–20, 1997), 363–367.

Book chapters

1. Goues, C. L., Nguyen-Tuong, A., **Chen**, **H.**, Davidson, J. W., Forrest, S., Hiser, J. D., Knight, J. C. & Van Gundy, M. in *Moving Target Defense II: Application of Game Theory and Adversarial Modeling* (ed et al., S. J.) 117–149 (Springer-Verlag New York, 2012).

PATENTS

1. Machiraju, S., Bolot, J. & Chen, H. US 9 503 895 (2016).
2. Machiraju, S., Bolot, J. & Chen, H. US 8 873 752 (2014).
3. Zang, H., Cai, L., Chen, H. & Maganis, G. US 8 639 275 (2014).
4. Zang, H., Cai, L., Chen, H. & Maganis, G. US 8 509 821 (2013).
5. Machiraju, S., Hsu, F. & Chen, H. US 8 442 527 (2013).
6. Hu, J., Sproeat, R. & Chen, H. US 6 373 985 (2002).
7. Hu, J., Sproeat, R. & Chen, H. US 6 360 010 (2002).