Big-4 Security Conference Papers: 2009, 2010, 2011

pvo

October 23, 2011

NDSS 2009

1. Document Structure Integrity: A Robust Basis for Cross-site Scripting Defense.
   Y. Nadji, P. Saxena, D. Song
2. An Efficient Black-box Technique for Defeating Web Application Attacks.
   R. Sekar
3. Noncespaces: Using Randomization to Enforce Information Flow Tracking and Thwart Cross-Site Scripting Attacks.
   M. Van Gundy, H. Chen
4. The Blind Stone Tablet: Outsourcing Durability to Untrusted Parties.
   P. Williams, R. Sion, D. Shasha
5. Two-Party Computation Model for Privacy-Preserving Queries over Distributed Databases.
   S.S.M. Chow, J.-H. Lee, L. Subramanian
6. SybilInfer: Detecting Sybil Nodes using Social Networks.
   G. Danezis, P. Mittal
7. Spectrogram: A Mixture-of-Markov-Chains Model for Anomaly Detection in Web Traffic.
   Yingbo Song, Angelos D. Keromytis, Salvatore J. Stolfo
8. Detecting Forged TCP Reset Packets.
   Nicholas Weaver, Robin Sommer, Vern Paxson
9. Coordinated Scan Detection.
   Carrie Gates
10. RB-Seeker: Auto-detection of Redirection Botnets.
    Xin Hu, Matthew Knysz, Kang G. Shin
11. Scalable, Behavior-Based Malware Clustering.
    Ulrich Bayer, Paolo Milani Comparetti, Clemens Hlauschek, Christopher Kruegel, Engin Kirda
12. K-Tracer: A System for Extracting Kernel Malware Behavior.
    Andrea Lanzi, Monirul I. Sharif, Wenke Lee
13. RAINBOW: A Robust And Invisible Non-Blind Watermark for Network Flows.
    Amir Houmansadr, Negar Kiyavash, Nikita Borisov
14. Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis.
    Charles V. Wright, Scott E. Coull, Fabian Monrose
15. Recursive DNS Architectures and Vulnerability Implications.
    David Dagon, Manos Antonakakis, Kevin Day, Xiapu Luo, Christopher P. Lee, Wenke Lee
16. Analyzing and Comparing the Protection Quality of Security Enhanced Operating Systems.
    Hong Chen, Ninghui Li, Ziqing Mao
17. IntScope: Automatically Detecting Integer Overflow Vulnerability in X86 Binary Using Symbolic Execution.
    Tielei Wang, Tao Wei, Zhiqiang Lin, Wei Zou
18. Safe Passage for Passwords and Other Sensitive Data.
    Jonathan M. McCune, Adrian Perrig, Michael K. Reiter
19. Conditioned-safe Ceremonies and a User Study of an Application to Web Authentication.
    Chris Karlof, J. Doug Tygar, David Wagner
20. CSAR: A Practical and Provable Technique to Make Randomized Systems Accountable.
    Michael Backes, Peter Druschel, Andreas Haeberlen, Dominique Unruh

Oakland 2009

1. Wirelessly Pickpocketing a Mifare Classic Card. (Best Practical Paper Award)
   Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur
2. Plaintext Recovery Attacks Against SSH.
   Martin R. Albrecht, Kenneth G. Paterson, Gaven J. Watson
3. Exploiting Unix File-System Races via Algorithmic Complexity Attacks.
   Xiang Cai, Yuwei Gui, Rob Johnson
4. Practical Mitigations for Timing-Based Side-Channel Attacks on Modern x86 Processors.
   Bart Coppens, Ingrid Verbauwhede, Bjorn De Sutter, Koen De Bosschere
5. Non-Interference for a Practical DIFC-Based Operating System.
   Maxwell Krohn, Eran Tromer
6. Native Client: A Sandbox for Portable, Untrusted x86 Native Code. (Best Paper Award)
   B. Yee, D. Sehr, G. Dardyk, B. Chen, R. Muth, T. Ormandy, S. Okasaka, N. Narula, N. Fullagar
7. Automatic Reverse Engineering of Malware Emulators. (Best Student Paper Award)
   Monirul Sharif, Andrea Lanzi, Jonathon Giffin, Wenke Lee
8. Prospex: Protocol Specification Extraction.
   Paolo Milani Comparetti, Gilbert Wondracek, Christopher Kruegel, Engin Kirda
9. Quantifying Information Leaks in Outbound Web Traffic.
   Kevin Borders, Atul Prakash
10. Automatic Discovery and Quantification of Information Leaks.
    Michael Backes, Boris Kopf, Andrey Rybalchenko
11. CLAMP: Practical Prevention of Large-Scale Data Leaks.
    Bryan Parno, Jonathan M. McCune, Dan Wendlandt, David G. Andersen, Adrian Perrig
12. De-anonymizing Social Networks.
    Arvind Narayanan, Vitaly Shmatikov
13. Privacy Weaknesses in Biometric Sketches.
    Koen Simoens, Pim Tuyls, Bart Preneel
14. The Mastermind Attack on Genomic Data.
    Michael T. Goodrich
15. A Logic of Secure Systems and its Application to Trusted Computing.
    Anupam Datta, Jason Franklin, Deepak Garg, Dilsun Kaynar
16. Formally Certifying the Security of Digital Signature Schemes.
    Santiago Zanella-Beguelin, Gilles Barthe, Benjamin Gregoire, Federico Olmedo
17. An Epistemic Approach to Coercion-Resistance for Electronic Voting Protocols.
    Ralf Kuesters, Tomasz Truderung
18. Sphinx: A Compact and Provably Secure Mix Format.
    George Danezis, Ian Goldberg
19. DSybil: Optimal Sybil-Resistance for Recommendation Systems.
    Haifeng Yu, Chenwei Shi, Michael Kaminsky, Phillip B. Gibbons, Feng Xiao
20. Fingerprinting Blank Paper Using Commodity Scanners.
    William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, Alex Halderman, Ed Felten
21. Tempest in a Teapot: Compromising Reflections Revisited.
    Michael Backes, Tongbo Chen, Markus Duermuth, Hendrik P. A. Lensch, Martin Welk
22. Blueprint: Robust Prevention of Cross-site Scripting Attacks for Existing Browsers.
    Mike Ter Louw, V.N. Venkatakrishnan
23. Pretty-Bad-Proxy: An Overlooked Adversary in Browsers' HTTPS Deployments.
    Shuo Chen, Ziqing Mao, Yi-Min Wang, Ming Zhang
24. Secure Content Sniffing for Web Browsers, or How to Stop Papers from Reviewing Themselves.
    Adam Barth, Juan Caballero, Dawn Song
25. It's No Secret: Measuring the Security and Reliability of Authentication via 'Secret' Questions.
    Stuart Schechter, A. J. Bernheim Brush, Serge Egelman
26. Password Cracking Using Probabilistic Context-Free Grammars.
    Matt Weir, Sudhir Aggarwal, Bill Glodek, Breno de Medeiros

USENIX Security 2009

1. Compromising Electromagnetic Emanations of Wired and Wireless Keyboards. (Outstanding Student Paper)
   Martin Vuagnoux, Sylvain Pasini
2. Peeping Tom in the Neighborhood: Keystroke Eavesdropping on Multi-User Systems.
   Kehuan Zhang, XiaoFeng Wang
3. A Practical Congestion Attack on Tor Using Long Paths,
   Nathan S. Evans, Roger Dingledine, Christian Grothoff
4. Baggy Bounds Checking: An Efficient and Backwards-Compatible Defense against Out-of-Bounds Errors.
   Periklis Akritidis, Manuel Costa, Miguel Castro, Steven Hand
5. Dynamic Test Generation to Find Integer Bugs in x86 Binary Linux Programs.
   David Molnar, Xue Cong Li, David A. Wagner
6. NOZZLE: A Defense Against Heap-spraying Code Injection Attacks.
   Paruj Ratanaworabhan, Benjamin Livshits, Benjamin Zorn
7. Detecting Spammers with SNARE: Spatio-temporal Network-level Automatic Reputation Engine.
   Shuang Hao, Nadeem Ahmed Syed, Nick Feamster, Alexander G. Gray, Sven Krasser
8. Improving Tor using a TCP-over-DTLS Tunnel.
   Joel Reardon, Ian Goldberg
9. Locating Prefix Hijackers using LOCK.
   Tongqing Qiu, Lusheng Ji, Dan Pei, Jia Wang, Jun (Jim) Xu, Hitesh Ballani
10. GATEKEEPER: Mostly Static Enforcement of Security and Reliability Policies for JavaScript Code.
    Salvatore Guarnieri, Benjamin Livshits
11. Cross-Origin JavaScript Capability Leaks: Detection, Exploitation, and Defense.
    Adam Barth, Joel Weinberger, Dawn Song
12. Memory Safety for Low-Level Software/Hardware Interactions.
    John Criswell, Nicolas Geoffray, Vikram Adve
13. Physical-layer Identification of RFID Devices.
    Boris Danev, Thomas S. Heydt-Benjamin, Srdjan Capkun
14. CCCP: Secure Remote Storage for Computational RFIDs.
    Mastooreh Salajegheh, Shane Clark, Benjamin Ransford, Kevin Fu, Ari Juels
15. Jamming-resistant Broadcast Communication without Shared Keys.
    Christina Popper, Mario Strasser, Srdjan Capkun
16. xBook: Redesigning Privacy Control in Social Networking Platforms.
    Kapil Singh, Sumeer Bhola, Wenke Lee
17. Nemesis: Preventing Authentication and Access Control Vulnerabilities in Web Applications.
    Michael Dalton, Christos Kozyrakis, Nickolai Zeldovich
18. Static Enforcement of Web Application Integrity Through Strong Typing.
    William Robertson, Giovanni Vigna
19. Vanish: Increasing Data Privacy with Self-Destructing Data. (Outstanding Student Paper)
    Roxana Geambasu, Tadayoshi Kohno, Amit A. Levy, Henry M. Levy
20. Efficient Data Structures for Tamper-Evident Logging.
    Scott A. Crosby, Dan S. Wallach
21. VPriv: Protecting Privacy in Location-Based Vehicular Services.
    Raluca Ada Popa, Hari Balakrishnan, Andrew J. Blumberg
22. Effective and Efficient Malware Detection at the End Host.
    Clemens Kolbitsch, Paolo Milani Comparetti, Christopher Kruegel, Engin Kirda, Xiaoyong Zhou, XiaoFeng Wang
23. Protecting Confidential Data on Personal Computers with Storage Capsules.
    Kevin Borders, Eric Vander Weele, Billy Lau, Atul Prakash
24. Return-Oriented Rootkits: Bypassing Kernel Code Integrity Protection Mechanisms.
    Ralf Hund, Thorsten Holz, Felix C. Freiling
25. Crying Wolf: An Empirical Study of SSL Warning Effectiveness.
    Joshua Sunshine, Serge Egelman, Hazim Almuhimedi, Neha Atri, Lorrie Faith Cranor
26. The Multi-Principal OS Construction of the Gazelle Web Browser.
    Helen J. Wang, Chris Grier, Alex Moshchuk, Samuel T. King, Piali Choudhury, Herman Venter

ACM CCS 2009

1. Attacking cryptographic schemes based on "perturbation polynomials".
   Martin Albrecht, Craig Gentry, Shai Halevi, Jonathan Katz
2. Filter-resistant code injection on ARM.
   Yves Younan, Pieter Philippaerts, Frank Piessens, Wouter Joosen, Sven Lachmund, Thomas Walter
3. False data injection attacks against state estimation in electric power grids.
   Yao Liu, Michael K. Reiter, Peng Ning
4. EPC RFID tag security weaknesses and defenses: passport cards, enhanced drivers licenses, and beyond.
   Karl Koscher, Ari Juels, Vjekoslav Brajkovic, Tadayoshi Kohno
5. An efficient forward private RFID protocol.
   Come Berbain, Olivier Billet, Jonathan Etrog, Henri Gilbert
6. RFID privacy: relation between two notions, minimal condition, and efficient construction.
   Changshe Ma, Yingjiu Li, Robert H. Deng, Tieyan Li
7. CoSP: a general framework for computational soundness proofs.
   Michael Backes, Dennis Hofheinz, Dominique Unruh
8. Reactive noninterference.
   Aaron Bohannon, Benjamin C. Pierce, Vilhelm Sjoberg, Stephanie Weirich, Steve Zdancewic
9. Computational soundness for key exchange protocols with symmetric encryption.
   Ralf Kusters, Max Tuengerthal
10. A probabilistic approach to hybrid role mining.
    Mario Frank, Andreas P. Streich, David A. Basin, Joachim M. Buhmann
11. Efficient pseudorandom functions from the decisional linear assumption and weaker variants.
    Allison B. Lewko, Brent Waters
12. Improving privacy and security in multi-authority attribute-based encryption.
    Melissa Chase, Sherman S. M. Chow
13. Oblivious transfer with access control.
    Jan Camenisch, Maria Dubovitskaya, Gregory Neven
14. NISAN: network information service for anonymization networks.
    Andriy Panchenko, Stefan Richter, Arne Rache
15. Certificateless onion routing.
    Dario Catalano, Dario Fiore, Rosario Gennaro
16. ShadowWalker: peer-to-peer anonymous communication using redundant structured topologies.
    Prateek Mittal, Nikita Borisov
17. Ripley: automatically securing web 2.0 applications through replicated execution.
    K. Vikram, Abhishek Prateek, V. Benjamin Livshits
18. HAIL: a high-availability and integrity layer for cloud storage.
    Kevin D. Bowers, Ari Juels, Alina Oprea
19. Hey, you, get off of my cloud: exploring information leakage in third-party compute clouds.
    Thomas Ristenpart, Eran Tromer, Hovav Shacham, Stefan Savage
20. Dynamic provable data possession.
    C. Christopher Erway, Alptekin Kupcu, Charalampos Papamanthou, Roberto Tamassia
21. On cellular botnets: measuring the impact of malicious devices on a cellular network core.
    Patrick Traynor, Michael Lin, Machigar Ongtang, Vikhyath Rao, Trent Jaeger, Patrick Drew McDaniel, Thomas F. La Porta
22. On lightweight mobile phone application certification.
    William Enck, Machigar Ongtang, Patrick Drew McDaniel
23. SMILE: encounter-based trust for mobile social services.
    Justin Manweiler, Ryan Scudellari, Landon P. Cox
24. Battle of Botcraft: fighting bots in online games with human observational proofs.
    Steven Gianvecchio, Zhenyu Wu, Mengjun Xie, Haining Wang
25. Fides: remote anomaly-based cheat detection using client emulation.
    Edward C. Kaiser, Wu-chang Feng, Travis Schluessler
26. Behavior based software theft detection.
    Xinran Wang, Yoon-chan Jhi, Sencun Zhu, Peng Liu
27. The fable of the bees: incentivizing robust revocation decision making in ad hoc networks.
    Steffen Reidt, Mudhakar Srivatsa, Shane Balfe
28. Effective implementation of the cell broadband engineTM isolation loader.
    Masana Murase, Kanna Shimizu, Wilfred Plouffe, Masaharu Sakamoto
29. On achieving good operating points on an ROC plane using stochastic anomaly score prediction.
    Muhammad Qasim Ali, Hassan Khan, Ali Sajjad, Syed Ali Khayam
30. On non-cooperative location privacy: a game-theoretic analysis.
    Julien Freudiger, Mohammad Hossein Manshaei, Jean-Pierre Hubaux, David C. Parkes
31. Privacy-preserving genomic computation through program specialization.
    Rui Wang, XiaoFeng Wang, Zhou Li, Haixu Tang, Michael K. Reiter, Zheng Dong

32. Feeling-based location privacy protection for location-based services.
    Toby Xu, Ying Cai
33. Multi-party off-the-record messaging.
    Ian Goldberg, Berkant Ustaoglu, Matthew Van Gundy, Hao Chen
34. The bayesian traffic analysis of mix networks.
    Carmela Troncoso, George Danezis
35. As-awareness in Tor path selection.
    Matthew Edman, Paul F. Syverson
36. Membership-concealing overlay networks.
    Eugene Y. Vasserman, Rob Jansen, James Tyra, Nicholas Hopper, Yongdae Kim
37. On the difficulty of software-based attestation of embedded devices.
    Claude Castelluccia, Aurelien Francillon, Daniele Perito, Claudio Soriente
38. Proximity-based access control for implantable medical devices.
    Kasper Bonne Rasmussen, Claude Castelluccia, Thomas S. Heydt-Benjamin, Srdjan Capkun
39. XCS: cross channel scripting and its impact on web applications.
    Hristo Bojinov, Elie Bursztein, Dan Boneh
40. A security-preserving compiler for distributed programs: from information-flow policies to cryptographic mechanisms.
    Cedric Fournet, Gurvan Le Guernic, Tamara Rezk
41. Finding bugs in exceptional situations of JNI programs.
    Siliang Li, Gang Tan
42. Secure open source collaboration: an empirical study of Linus' law.
    Andrew Meneely, Laurie A. Williams
43. On voting machine design for verification and testability.
    Cynthia Sturton, Susmit Jha, Sanjit A. Seshia, David Wagner
44. Secure in-VM monitoring using hardware virtualization.
    Monirul I. Sharif, Wenke Lee, Weidong Cui, Andrea Lanzi
45. A metadata calculus for secure information sharing.
    Mudhakar Srivatsa, Dakshi Agrawal, Steffen Reidt
46. Multiple password interference in text passwords and click-based graphical passwords.
    Sonia Chiasson, Alain Forget, Elizabeth Stobert, Paul C. van Oorschot, Robert Biddle
47. Can they hear me now?: a security analysis of law enforcement wiretaps.
    Micah Sherr, Gaurav Shah, Eric Cronin, Sandy Clark, Matt Blaze
48. English shellcode.
    Joshua Mason, Sam Small, Fabian Monrose, Greg MacManus
49. Learning your identity and disease from research papers: information leaks in genome wide association study.
    Rui Wang, Yong Fuga Li, XiaoFeng Wang, Haixu Tang, Xiao-yong Zhou
50. Countering kernel rootkits with lightweight hook protection.
    Zhi Wang, Xuxian Jiang, Weidong Cui, Peng Ning
51. Mapping kernel objects to enable systematic integrity checking.
    Martim Carbone, Weidong Cui, Long Lu, Wenke Lee, Marcus Peinado, Xuxian Jiang
52. Robust signatures for kernel data structures.
    Brendan Dolan-Gavitt, Abhinav Srivastava, Patrick Traynor, Jonathon T. Giffin
53. A new cell counter based attack against tor.
    Zhen Ling, Junzhou Luo, Wei Yu, Xinwen Fu, Dong Xuan, Weijia Jia
54. Scalable onion routing with torsk.
    Jon McLachlan, Andrew Tran, Nicholas Hopper, Yongdae Kim
55. Anonymous credentials on a standard java card.
    Patrik Bichsel, Jan Camenisch, Thomas Gros, Victor Shoup
56. Large-scale malware indexing using function-call graphs.
    Xin Hu, Tzi-cker Chiueh, Kang G. Shin
57. Dispatcher: enabling active botnet infiltration using automatic protocol reverse-engineering.
    Juan Caballero, Pongsin Poosankam, Christian Kreibich, Dawn Xiaodong Song
58. Your botnet is my botnet: analysis of a botnet takeover. Brett Stone-Gross, Marco Cova, Lorenzo Cavallaro, Bob Gilbert, Martin Szydlowski, Richard A. Kemmerer, Christopher Kruegel, Giovanni Vigna

NDSS 2010

1. Server-side Verification of Client Behavior in Online Games.
   Darrell Bethea, Robert Cochran and Michael Reiter
2. Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs.
   S. Wolchok, O.S. Hofmann, N. Heninger, E.W. Felten, J.A. Halderman, C.J. Rossbach, B. Waters, E. Witchel
3. Stealth DoS Attacks on Secure Channels.
   Amir Herzberg and Haya Shulman
4. Protecting Browsers from Extension Vulnerabilities.
   Adam Barth, Adrienne Porter Felt, Prateek Saxena, and Aaron Boodman
5. Adnostic: Privacy Preserving Targeted Advertising.
   Vincent Toubiana, Arvind Narayanan, Dan Boneh, Helen Nissenbaum and Solon Barocas
6. FLAX: Systematic Discovery of Client-side Validation Vulnerabilities in Rich Web Applications.
   Prateek Saxena, Steve Hanna, Pongsin Poosankam and Dawn Song
7. Effective Anomaly Detection with Scarce Training Data.
   William Robertson, Federico Maggi, Christopher Kruegel and Giovanni Vigna
8. Large-Scale Automatic Classification of Phishing Pages.
   Colin Whittaker, Brian Ryner and Marria Nazif
9. A Systematic Characterization of IM Threats using Honeypots.
   Iasonas Polakis, Thanasis Petsas, Evangelos P. Markatos and Spiros Antonatos
10. On Network-level Clusters for Spam Detection.
    Zhiyun Qian, Zhuoqing Mao, Yinglian Xie and Fang Yu
11. Improving Spam Blacklisting Through Dynamic Thresholding and Speculative Aggregation.
    Sushant Sinha, Michael Bailey and Farnam Jahanian
12. Botnet Judo: Fighting Spam with Itself.
    A. Pitsillidis, K. Levchenko, C. Kreibich, C. Kanich, G.M. Voelker, V. Paxson, N. Weaver, S. Savage
13. Contractual Anonymity.
    Edward J. Schwartz, David Brumley and Jonathan M. McCune
14. A3: An Extensible Platform for Application-Aware Anonymity.
    Micah Sherr, Andrew Mao, William R. Marczak, Wenchao Zhou, Boon Thau Loo, and Matt Blaze
15. When Good Randomness Goes Bad: Virtual Machine Reset Vulnerabilities and Hedging Deployed Cryptography.
    Thomas Ristenpart and Scott Yilek
16. InvisiType: Object-Oriented Security Policies.
    Jiwon Seo and Monica S. Lam
17. A Security Evaluation of DNSSEC with NSEC3.
    Jason Bau and John Mitchell
18. On the Safety of Enterprise Policy Deployment.
    Yudong Gao, Ni Pan, Xu Chen and Z. Morley Mao
19. Where Do You Want to Go Today? Escalating Privileges by Pathname Manipulation.
    Suresh Chari, Shai Halevi and Wietse Venema
20. Joe-E: A Security-Oriented Subset of Java.
    Adrian Mettler, David Wagner and Tyler Close
21. Preventing Capability Leaks in Secure JavaScript Subsets.
    Matthew Finifter, Joel Weinberger and Adam Barth
22. Binary Code Extraction and Interface Identification for Security Applications.
    Juan Caballero, Noah M. Johnson, Stephen McCamant, and Dawn Song
23. Automatic Reverse Engineering of Data Structures from Binary Execution.
    Zhiqiang Lin, Xiangyu Zhang and Dongyan Xu
24. Efficient Detection of Split Personalities in Malware.
    Davide Balzarotti, Marco Cova, Christoph Karlberger, Engin Kirda, Christopher Kruegel and Giovanni Vigna

Oakland 2010

1. Inspector Gadget: Automated Extraction of Proprietary Gadgets from Malware Binaries.
   Clemens Kolbitsch Thorsten Holz, Christopher Kruegel, Engin Kirda
2. Synthesizing Near-Optimal Malware Specifications from Suspicious Behaviors.
   Matt Fredrikson, Mihai Christodorescu, Somesh Jha, Reiner Sailer, Xifeng Yan
3. Identifying Dormant Functionality in Malware Programs.
   Paolo Milani Comparetti, Guido Salvaneschi, Clemens Kolbitsch, Engin Kirda, Christopher Kruegel, Stefano Zanero
4. Reconciling Belief and Vulnerability in Information Flow.
   Sardaouna Hamadou, Vladimiro Sassone, Palamidessi
5. Towards Static Flow-Based Declassification for Legacy and Untrusted Programs.
   Bruno P.S. Rocha, Sruthi Bandhakavi, Jerry I. den Hartog, William H. Winsborough, Sandro Etalle
6. Non-Interference Through Secure Multi-Execution.
   Dominique Devriese, Frank Piessens
7. Object Capabilities and Isolation of Untrusted Web Applications.
   Sergio Maffeis, John C. Mitchell, Ankur Taly
8. TrustVisor: Efficient TCB Reduction and Attestation.
   Jonathan McCune, Yanlin Li, Ning Qu, Zongwei Zhou, Anupam Datta, Virgil Gligor, Adrian Perrig
9. Overcoming an Untrusted Computing Base: Detecting and Removing Malicious Hardware Automatically.
   Matthew Hicks, Murph Finnicum, Samuel T. King, Milo M. K. Martin,Jonathan M. Smith
10. Tamper Evident Microprocessors.
    Adam Waksman, Simha Sethumadhavan
11. Side-Channel Leaks in Web Applications: a Reality Today, a Challenge Tomorrow.
    Shuo Chen, Rui Wang, XiaoFeng Wang Kehuan Zhang
12. Investigation of Triangular Spamming: a Stealthy and Efficient Spamming Technique.
    Zhiyun Qian, Z. Morley Mao, Yinglian Xie, Fang Yu
13. A Practical Attack to De-Anonymize Social Network Users.
    Gilbert Wondracek, Thorsten Holz, Engin Kirda, Christopher Kruegel
14. SCiFI - A System for Secure Face Identification. (Best Paper)
    Margarita Osadchy, Benny Pinkas, Ayman Jarrous, Boaz Moskovich
15. Round-Efficient Broadcast Authentication Protocols for Fixed Topology Classes.
    Haowen Chan, Adrian Perrig
16. Revocation Systems with Very Small Private Keys.
    Allison Lewko, Amit Sahai, Brent Waters
17. Authenticating Primary Users' Signals in Cognitive Radio Networks via Integrated Cryptographic and Wireless Link Signatures.
    Yao Liu, Peng Ning, Huaiyu Dai
18. Outside the Closed World: On Using Machine Learning For Network Intrusion Detection.
    Robin Sommer, Vern Paxson
19. All You Ever Wanted to Know about Dynamic Taint Analysis and Forward Symbolic Execution
    (but might have been afraid to ask). Thanassis Avgerinos, Edward Schwartz, David Brumley
20. State of the Art: Automated Black-Box Web Application Vulnerability Testing.
    Jason Bau, Elie Bursztein, Divij Gupta, John Mitchell
21. A Proof-Carrying File System.
    Deepak Garg, Frank Pfenning
22. Scalable Parametric Verification of Secure Systems: How to Verify Ref. Monitors without Worrying about Data Structure Size.
    Jason Franklin, Sagar Chaki, Anupam Datta, Arvind Seshadri
23. HyperSafe: A Lightweight Approach to Provide Lifetime Hypervisor Control-Flow Integrity.
    Zhi Wang, Xuxian Jiang
24. How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation.
    Elie Bursztein, Steven Bethard, John C. Mitchell, Dan Jurafsky, Celine Fabry
25. Bootstrapping Trust in Commodity Computers.
    Bryan Parno, Jonathan M. McCune, Adrian Perrig
26. Chip and PIN is Broken. (Best Practical Paper)
    Steven J. Murdoch, Saar Drimer, Ross Anderson, Mike Bond
27. Experimental Security Analysis of a Modern Automobile.
    K.Koscher, A.Czeskis, F.Roesner, S.Patel, T.Kohno, S.Checkoway, D.McCoy, B.Kantor, D.Anderson, H.Shacham, S.Savage
28. On the Incoherencies in Web Browser Access Control Policies.
    Kapil Singh, Alexander Moshchuk, Helen J. Wang, Wenke Lee
29. ConScript: Specifying and Enforcing Fine-Grained Security Policies for JavaScript in the Browser.
    Leo Meyerovich, Benjamin Livshits
30. TaintScope: A Checksum-Aware Directed Fuzzing Tool for Automatic Software Vulnerability Detection. (Best Student Paper)
    Tielei Wang, Tao Wei, Guofei Gu, Wei Zou
31. A Symbolic Execution Framework for JavaScript.
    Prateek Saxena, Devdatta Akhawe, Steve Hanna, Stephen McCamant, Dawn Song, Feng Mao

USENIX Security 2010

1. Adapting Software Fault Isolation to Contemporary CPU Architectures.
   David Sehr, Robert Muth, Cliff Biffle, Victor Khimenko, Egor Pasko, Karl Schimpf, Bennet Yee, Brad Chen
2. Making Linux Protection Mechanisms Egalitarian with UserFS.
   Taesoo Kim and Nickolai Zeldovich
3. Capsicum: Practical Capabilities for UNIX. (Best Student Paper)
   Robert N.M. Watson, Jonathan Anderson, Ben Laurie, Kris Kennaway
4. Structuring Protocol Implementations to Protect Sensitive Data.
   Petr Marchenko, Brad Karp
5. PrETP: Privacy-Preserving Electronic Toll Pricing.
   Josep Balasch, Alfredo Rial, Carmela Troncoso, Bart Preneel, Ingrid Verbauwhede, Christophe Geuens
6. An Analysis of Private Browsing Modes in Modern Browsers.
   Gaurav Aggarwal, Elie Bursztein, Collin Jackson, Dan Boneh
7. BotGrep: Finding P2P Bots with Structured Graph Analysis.
   Shishir Nagaraja, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, Nikita Borisov
8. Fast Regular Expression Matching Using Small TCAMs for Network Intrusion Detection and Prevention Systems.
   Chad R. Meiners, Jignesh Patel, Eric Norige, Eric Torng, Alex X. Liu
9. Searching the Searchers with SearchAudit.
   John P. John, Fang Yu, Yinglian Xie, Martin Abadi, Arvind Krishnamurthy
10. Toward Automated Detection of Logic Vulnerabilities in Web Applications.
    Viktoria Felmetsger, Ludovico Cavedon, Christopher Kruegel, Giovanni Vigna
11. Baaz: A System for Detecting Access Control Misconfigurations.
    Tathagata Das, Ranjita Bhagwan, Prasad Naldurg
12. Cling: A Memory Allocator to Mitigate Dangling Pointers.
    Periklis Akritidis
13. ZKPDL: A Language-Based System for Efficient Zero-Knowledge Proofs and Electronic Cash.
    Sarah Meiklejohn, C. Chris Erway, Alptekin Kupcu, Theodora Hinkle, Anna Lysyanskaya
14. P4P: Practical Large-Scale Privacy-Preserving Distributed Computation Robust against Malicious Users.
    Yitao Duan, John Canny, Justin Zhan,
15. SEPIA: Privacy-Preserving Aggregation of Multi-Domain Network Events and Statistics.
    Martin Burkhart, Mario Strasser, Dilip Many, Xenofontas Dimitropoulos
16. Dude, Where's That IP? Circumventing Measurement-based IP Geolocation.
    Phillipa Gill, Yashar Ganjali, Bernard Wong, David Lie
17. Idle Port Scanning and Non-interference Analysis of Network Protocol Stacks Using Model Checking.
    Roya Ensafi, Jong Chun Park, Deepak Kapur, Jedidiah R. Crandall
18. Building a Dynamic Reputation System for DNS.
    Manos Antonakakis, Roberto Perdisci, David Dagon, Wenke Lee, Nick Feamster
19. Scantegrity II Municipal Election at Takoma Park: The First E2E Binding Governmental Election with Ballot Privacy. R.Carback, D.Chaum, J.Clark, J.Conway, A.Essex, P.S.Herrnson, T.Mayberry, S.Popoveniuc, R.L.Rivest, E.Shen, A.T.Sherman, P.L. Vora
20. Acoustic Side-Channel Attacks on Printers.
    Michael Backes, Markus Durmuth, Sebastian Gerling, Manfred Pinkal, Caroline Sporleder
21. Security and Privacy Vulnerabilities of In-Car Wireless Networks: A Tire Pressure Monitoring System Case Study.
    Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor, Sangho Oh, Wenyuan Xu, Marco Gruteser, Wade Trappe, Ivan Seskar
22. VEX: Vetting Browser Extensions for Security Vulnerabilities. (Best Paper)
    Sruthi Bandhakavi, Samuel T. King, P. Madhusudan, Marianne Winslett
23. Securing Script-Based Extensibility in Web Browsers.
    Vladan Djeric, Ashvin Goel
24. AdJail: Practical Enforcement of Confidentiality and Integrity Policies on Web Advertisements.
    Mike Ter Louw, Karthik Thotta Ganesh, V.N. Venkatakrishnan
25. Realization of RF Distance Bounding.
    Kasper Bonne Rasmussen, Srdjan Capkun
26. The Case for Ubiquitous Transport-Level Encryption.
    Andrea Bittau, Michael Hamburg, Mark Handley, David Mazieres, Dan Boneh
27. Automatic Generation of Remediation Procedures for Malware Infections.
    Roberto Paleari, Lorenzo Martignoni, Emanuele Passerini, Drew Davidson, Matt Fredrikson, Jon Giffin, Somesh Jha
28. Re: CAPTCHAs-Understanding CAPTCHA-Solving Services in an Economic Context.
    Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker, Stefan Savage
29. Chipping Away at Censorship Firewalls with User-Generated Content.
    Sam Burnett, Nick Feamster, Santosh Vempala
30. Fighting Coercion Attacks in Key Generation using Skin Conductance.
    Payas Gupta, Debin Gao

ACM CCS 2010

1. Security Analysis of India's Electronic Voting Machines.
   Scott Wolchok, Erik Wustrow, J. Alex Halderman, Hari Prasad, Rop Gonggrijp
2. Dissecting One Click Frauds.
   Nicolas Christin, Sally S. Yanagihara, Keisuke Kamataki
3. @spam: The Underground on 140 Characters or Less.
   Chris Grier, Kurt Thomas, Vern Paxson, Michael Zhang
4. HyperSentry: Enabling Stealthy In-context Measurement of Hypervisor Integrity.
   Ahmed M. Azab, Peng Ning, Zhi Wang, Xuxian Jiang, Xiaolan Zhang, Nathan C. Skalsky
5. Trail of Bytes: Efficient Support for Forensic Analysis.
   Srinivas Krishnan, Kevin Z. Snow, Fabian Monrose
6. Survivable Key Compromise in Software Update Systems.
   Justin Samuel, Nick Mathewson, Justin Cappos, Roger Dingledine
7. A Methodology for Empirical Analysis of the Permission-Based Security Models and its Application to Android.
   David Barrera, H. Gunes Kayacik, Paul C. van Oorschot, Anil Somayaji
8. Mobile Location Tracking in Metropolitan Areas: malnets and others.
   Nathanial Husted, Steve Myers
9. On Pairing Constrained Wireless Devices Based on Secrecy of Auxiliary Channels: The Case of Acoustic Eavesdropping.
   Tzipora Halevi, Nitesh Saxena
10. PinDr0p: Using Single-Ended Audio Features to Determine Call Provenance.
    Vijay A. Balasubramaniyan, Aamir Poonawalla, Mustaque Ahamad, Michael T. Hunter, Patrick Traynor
11. Building Efficient Fully Collusion-Resilient Traitor Tracing and Revocation Schemes.
    Sanjam Garg, Abishek Kumarasubramanian, Amit Sahai, Brent Waters
12. Algebraic Pseudorandom Functions with Improved Efficiency from the Augmented Cascade.
    Dan Boneh, Hart Montgomery, Ananth Raghunathan
13. Practical Leakage-Resilient Pseudorandom Generators.
    Yu Yu, Francois-Xavier Standaert, Olivier Pereira, Moti Yung
14. Practical Leakage-Resilient Identity-Based Encryption from Simple Assumptions.
    Sherman S.M. Chow, Yevgeniy Dodis, Yannis Rouselakis, Brent Waters
15. Testing Metrics for Password Creation Policies by Attacking Large Sets of Revealed Passwords.
    Matt Weir, Sudhir Aggarwal, Michael Collins, Henry Stern
16. The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis.
    Yinqian Zhang, Fabian Monrose, Michael K. Reiter
17. Attacks and Design of Image Recognition CAPTCHAs.
    Bin Zhu, Jeff Yan, Chao Yang, Qiujie Li, Jiu Liu, Ning Xu, Meng Yi
18. Robusta: Taming the Native Beast of the JVM.
    Joseph Siefers, Gang Tan, Greg Morrisett
19. Retaining Sandbox Containment Despite Bugs in Privileged Memory-Safe Code. Justin Cappos, Armon Dadgar, Jeff Rasley, Justin Samuel, Ivan Beschastnikh, Cosmin Barsan, Arvind Krishnamurthy, Thomas Anderson
20. A Control Point for Reducing Root Abuse of File-System Privileges.
    Glenn Wurster, Paul C. van Oorschot
21. Modeling Attacks on Physical Unclonable Functions.
    Ulrich Ruehrmair, Frank Sehnke, Jan Soelter, Gideon Dror, Srinivas Devadas, Juergen Schmidhuber
22. Dismantling SecureMemory, CryptoMemory and CryptoRF.
    Flavio D. Garcia, Peter van Rossum, Roel Verdult, Ronny Wichers Schreur
23. Attacking and Fixing PKCS#11 Security Tokens.
    Matteo Bortolozzo, Matteo Centenaro, Riccardo Focardi, Graham Steel
24. An Empirical Study of Privacy-Violating Information Flows in JavaScript Web Applications.
    Dongseok Jang, Ranjit Jhala, Sorin Lerner, Hovav Shacham
25. DIFC Programs by Automatic Instrumentation.
    William Harris, Somesh Jha, Thomas Reps
26. Predictive Black-box Mitigation of Timing Channels.
    Aslan Askarov, Danfeng Zhang, Andrew Myers
27. In Search of an Anonymous and Secure Lookup: Attacks on Structured Peer-to-peer Anonymous Communication Systems.
    Qiyan Wang, Prateek Mittal, Nikita Borisov
28. Recruiting New Tor Relays with BRAIDS.
    Rob Jansen, Nicholas Hopper, Yongdae Kim
29. An Improved Algorithm for Tor Circuit Scheduling.
    Can Tang, Ian Goldberg
30. Dissent: Accountable Anonymous Group Messaging.
    Henry Corrigan-Gibbs, Bryan Ford
31. Abstraction by Set-Membership—Verifying Security Protocols and Web Services with Databases.
    Sebastian Moedersheim

32. Developing Security Protocols by Refinement.
    Christoph Sprenger, David Basin
33. Computational Indistinguishability Logic.
    Gilles Barthe, Marion Daubignard, Bruce Kapron, Yassine Lakhnech
34. Computationally Sound Verification of Source Code.
    Michael Backes, Matteo Maffei, Dominique Unruh
35. BLADE: An Attack-Agnostic Approach for Preventing Drive-By Malware Infections.
    Long Lu, Vinod Yegneswaran, Phillip Porras, Wenke Lee
36. AccessMiner: Using System-Centric Models for Malware Protection.
    Andrea Lanzi, Davide Balzarotti, Christopher Kruegel, Mihai Christodorescu, Engin Kirda
37. Input Generation via Decomposition and Re-Stitching: Finding Bugs in Malware.
    Juan Caballero, Pongsin Poosankam, Stephen McCamant, Domagoj Babic, Dawn Song
38. Inference and Analysis of Formal Models of Botnet Command and Control Protocols.
    Chia Yuan Cho, Domagoj Babic, Eui Chul Richard Shin, Dawn Song
39. TASTY: Tool for Automating Secure Two-partY computations.
    Wilko Henecka, Stefan Koegl, Ahmad-Reza Sadeghi, Thomas Schneider, Immo Wehrenberg
40. Worry-Free Encryption: Functional Encryption with Public Keys.
    Hakan Seyalioglu, Amit Sahai
41. Synchronized Aggregate Signatures.
    Jae Hyun Ahn, Matthew Green, Susan Hohenberger
42. Secure Text Processing with Applications to Private DNA Matching.
    Lior Malka, Jonathan Katz
43. On the (In)Security of IPsec in MAC-then-Encrypt Configurations.
    Jean Paul Degabriele, Kenneth G. Paterson
44. On the Soundness of Authenticate-then-Encrypt: Formalizing the Malleability of Symmetric Encryption.
    Ueli Maurer, Bjoern Tackmann
45. A New Framework for Efficient Password-Based Authenticated Key Exchange.
    Adam Groce, Jonathan Katz
46. Accountability: Definition and Relationship to Verifiability.
    Ralf Kuesters, Tomasz Truderung, Andreas Vogt
47. Mimimorphism: A New Approach to Binary Code Obfuscation.
    Zhenyu Wu, Steven Gianvecchio, Mengjun Xie, Haining Wang
48. Platform-Independent Program.
    Sang Kil Cha, Brian Pak, David Brumley, Richard J. Lipton
49. Return-Oriented Programming Without Returns.
    Stephen Checkoway, Lucas Davi, Alexandra Dmitrienko, Ahmad-Reza Sadeghi, Hovav Shacham, Marcel Winandy
50. DieHarder: Securing the Heap.
    Gene Novark, Emery D. Berger
51. Symbolic Security Analysis of Ruby-on-Rails Web Applications.
    Avik Chaudhuri, Jeffrey S. Foster
52. Sidebuster: Automated Detection and Quantification of Side-Channel Leaks in Web Application Development.
    Kehuan Zhang, Zhou Li, Rui Wang, XiaoFeng Wang, Shuo Chen
53. NoTamper: Automated Blackbox Detection of Parameter Tampering Opportunities in Web Applications.
    Prithvi Bisht , Timothy Hinrichs, Nazari Skrupsky, Radoslaw Bobrowicz, V.N. Venkatakrishnan
54. Protecting Browsers from Cross-Origin CSS Attacks.
    Lin-Shung Huang, Zack Weinberg, Chris Evans, Collin Jackson

NDSS 2011

1. Soundcomber: A Stealthy and Context-Aware Sound Trojan for Smartphones.
   R. Schlegel, K. Zhang, X. Zhou, M. Intwala, A. Kapadia, X. Wang
2. A Security API for Distributed Social Networks.
   M. Backes, M. Maffei, K. Pecina
3. Location Privacy via Private Proximity Testing.
   A. Narayanan, N. Thiagarajan, M. Lakhani, M. Hamburg, D. Boneh
4. Relay Attacks on Passive Keyless Entry and Start Systems in Modern Cars.
   A. Francillon, B. Danev, S. Capkun
5. Using Classification to Protect the Integrity of Spectrum Measurements in White Space Networks.
   O. Fatemieh, A. Farhadi, R. Chandra, C.A. Gunter
6. Good Neighbor: Ad hoc Pairing of Nearby Wireless Devices by Multiple Antennas.
   L. Cai, K. Zeng, H. Chen, P. Mohapatra
7. Practical Protection of Kernel Integrity for Commodity OS from Untrusted Extensions.
   X. Xiong, D. Tian, P. Liu
8. Efficient Monitoring of Untrusted Kernel-Mode Execution.
   A. Srivastava, J. Giffin
9. SigGraph: Brute Force Scanning of Kernel Data Structure Instances Using Graph-based Signatures.
   Z. Lin, J. Rhee, X. Zhang, D. Xu, X. Jiang
10. Losing Control of the Internet: Using the Data Plane to Attack the Control Plane.
    M. Schuchard, A. Mohaisen, D.F. Kune, N. Hopper, Y. Kim, E.Y. Vasserman
11. EXPOSURE: Finding Malicious Domains Using Passive DNS Analysis.
    L. Bilge, E. Kirda, C. Kruegel, M. Balduzzi
12. Howard: A Dynamic Excavator for Reverse Engineering Data Structures.
    A. Slowinska, T. Stancescu, H. Bos
13. No Loitering: Exploiting Lingering Vulnerabilities in Default COM Objects.
    D. Dewey, P. Traynor
14. TIE: Principled Reverse Engineering of Types in Binary Programs.
    J. Lee, T. Avgerinos, D. Brumley
15. DTA++: Dynamic Taint Analysis with Targeted Control-Flow Propagation.
    M.G. Kang, S. McCamant, P. Poosankam, D. Song
16. AEG: Automatic Exploit Generation.
    T. Avgerinos, S.K. Cha, B. Lim, T. Hao, D. Brumley
17. Automated Discovery of Parameter Pollution Vulnerabilities in Web Applications.
    M. Balduzzi, C.T. Gimenez, D. Balzarotti, E. Kirda
18. WebShield: Enabling Various Web Defense Techniques without Client Side Modifications.
    Z. Li, Y. Tang, Y. Cao, V. Rastogi, Y. Chen, B. Liu, C. Sbisa
19. HTTPOS: Sealing Information Leaks with Browser-side Obfuscation of Encrypted Flows.
    X. Luo, P. Zhou, E.W.W. Chan, W. Lee, R.K.C. Chang, R. Perdisci
20. Accurate and Provably Secure Latency Estimation with Treeple.
    E. Chan-Tin, N. Hopper
21. On Measuring the Similarity of Network Hosts: Pitfalls, New Metrics, and Empirical Analyses.
    S. Coull, F. Monrose, M. Bailey
22. SWIRL: A Scalable Watermark to Detect Correlated Network Flows.
    A. Houmansadr, N. Borisov
23. SPARE: Replicas on Hold.
    T. Distler, I. Popov, W. Schroder-Preikschat, H.P. Reiser, R. Kapitza
24. Efficient Privacy-Preserving Biometric Identification.
    Y. Huang, L. Malka, D. Evans, J. Katz
25. Usability Testing a Malware-Resistant Input Mechanism.
    A. Libonati, J.M. McCune, M.K. Reiter
26. Tracker: Security and Privacy for RFID-based Supply Chains.
    E.-O. Blass, K. Elkhiyaoui, R. Molva
27. PiOS: Detecting Privacy Leaks in iOS Applications.
    M. Egele, C. Kruegel, E. Kirda, G. Vigna
28. Privacy-Preserving Aggregation of Time-Series Data.
    E. Shi, T-H. Hubert Chan, E. Rieffel, R. Chow, D. Song

Oakland 2011

1. Hookt on fon-iks: Phonotactic Reconstruction of Encrypted VoIP Conversations.
   A.M. White, K. Snow, A. Matthews, F. Monrose
2. The Failure of Noise-Based Non-Continuous Audio Captchas.
   E. Bursztein, R. Beauxis, H.S. Paskov, D. Perito, C. Fabry, J.C. Mitchell
3. Using Fingerprint Authentication to Reduce System Security: An Empirical Study.
   Hugh Wimberly, Lorie M. Liebrock
4. Silencing Hardware Backdoors.
   A. Waksman, S. Sethumadhavan
5. Defeating UCI: Building Stealthy and Malicious Hardware.
   C. Sturton, M. Hicks, D. Wagner, S.T. King
6. Formalizing Anonymous Blacklisting Systems.
   R. Henry, I. Goldberg
7. Mobile Security Catching Up? Revealing the nuts and bolts of the security of mobile devices.
   M. Becher, F.C. Freiling, J. Hoffmann, T. Holz, S. Uellenbeck, C. Wolf
8. Verified Security for Browser Extensions.
   A. Guha, M. Fredrikson, B. Livshits, N. Swamy
9. RePriv: Re-Imagining Content Personalization and In-Browser Privacy.
   M. Fredrikson, B. Livshits
10. I Still Know What You Visited Last Summer: User interaction and side-channel attacks on browsing history.
    Z. Weinberg, E.Y. Chen, P. Ramesh Jayaraman, C. Jackson
11. Verification of Information Flow and Access Control Policies via Dependent Types.
    A. Nanevski, A. Banerjee, D. Garg
12. Inference of expressive declassification policies.
    J. Vaughan, S. Chong
13. The Complexity of Intransitive Noninterference.
    S. Eggert, R. van der Meyden, H. Schnoor, T. Wilke
14. SCION: Scalability, Control, and Isolation On Next-Generation Networks.
    X. Zhang, H.-C. Hsiao, G. Hasker, H. Chan, A. Perrig, D. Andersen
15. "You Might Also Like:" Privacy Risks of Collaborative Filtering.
    J.A. Calandrino, A. Kilzer, A. Narayanan, E.W. Felten, V. Shmatikov
16. Quantifying Location Privacy.
    R. Shokri, G. Theodorakopoulos, J.-Y. Le Boudec, J.-P. Hubaux
17. Preventing Sybil Attacks by Privilege Attenuation: A Design Principle for Social Network Systems.
    P.W.L. Fong
18. PRISM: Program Replication and Integration for Seamless MILS.
    C. Owen, D. Grove, T. Newby, A. Murray, C. North, M. Pope
19. Virtuoso: Narrowing the Semantic Gap in Virtual Machine Introspection.
    B. Dolan-Gavitt, T. Leek, M. Zhivich, J. Giffin, W. Lee
20. HomeAlone: Co-Residency Detection in the Cloud via Side-Channel Analysis.
    Y. Zhang, A. Juels, A. Oprea, M.K. Reiter
21. TxBox: Building Secure, Efficient Sandboxes with System Transactions.
    S. Jana, V. Shmatikov, D.E. Porter
22. Differential Slicing: Identifying Causal Execution Differences for Security Applications.
    N. Johnson, J. Caballero, K. Chen, S. McCamant, P. Poosankam, D. Reynaud, D. Song
23. Automated Analysis of Security-Critical JavaScript APIs.
    A. Taly, U. Erlingsson, M. Miller, J. C. Mitchell, J. Nagra
24. Memoir: Practical State Continuity for Protected Modules.
    B. Parno, J.R. Lorch, J.R. Douceur, J. Mickens, J.M. McCune
25. A Formal Foundation for the Security Features of Physical Functions.
    F. Armknecht, R. Maes, A.-R. Sadeghi, F.-X. Standaert, C. Wachsmann
26. Timing- and Termination-Sensitive Secure Information Flow: Exploring a New Approach.
    V. Kashyap, B. Wiedermann, B. Hardekopf
27. Click Trajectories: End-to-End Analysis of the Spam Value Chain.
    K. Levchenko, A. Pitsillidis, N. Chachra, B. Enright, M. Felegyhazi, C. Grier, T. Halvorson, C. Kanich, C. Kreibich, H. Liu, D. McCoy, N. Weaver, V. Paxson, G.M. Voelker, S. Savage
28. Design and Evaluation of a Real-Time URL Spam Filtering Service.
    K. Thomas, C. Grier, J. Ma, V. Paxson, D. Song
29. How to Shop for Free Online - Security Analysis of Cashier-as-a-Service Based Web Stores.
    R. Wang, S. Chen, X. Wang, S. Qadeer
30. Cryptography in the Web: The Case of Cryptographic Design Flaws in ASP.NET.
    T. Duong, J. Rizzo
31. Cache Games - Bringing Access-Based Cache Attacks on AES to Practice.
    E. Bangerter, D. Gullasch, S. Krenn

32. OpenConflict: Preventing Real Time Map Hacks in Online Games.
    E. Bursztein, M. Hamburg, J. Lagarenne, D. Boneh
33. Extending Nymble-like Systems.
    R. Henry, I. Goldberg
34. Verifiability, Privacy, and Coercion-Resistance: New Insights from a Case Study.
    R. Kuesters, T. Truderung, A. Vogt

USENIX Security 2011

1. Fast and Precise Sanitizer Analysis with BEK.
   P. Hooimeijer, B. Livshits, David Molnar, P. Saxena, M. Veanes
2. Toward Secure Embedded Web Interfaces.
   B. Gourdin, C. Soman, H. Bojinov, E. Bursztein
3. ZOZZLE: Fast and Precise In-Browser JavaScript Malware Detection.
   C. Curtsinger, B. Livshits, B. Zorn, C. Seifert
4. Why (Special Agent) Johnny (Still) Can't Encrypt: A Security Analysis of the APCO Project 25 Two-Way Radio System.
   (Outstanding Paper Award) S. Clark, T. Goodspeed, P. Metzger, Z. Wasserman, K. Xu, M. Blaze
5. Dark Clouds on the Horizon: Using Cloud Storage as Attack Vector and Online Slack Space.
   M. Mulazzani, S. Schrittwieser, M. Leithner, M. Huber, E. Weippl
6. Comprehensive Experimental Analyses of Automotive Attack Surfaces.
   S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno
7. Forensic Triage for Mobile Phones with DEC0DE.
   R.J. Walls, E. Learned-Miller, B.N. Levine
8. mCarve: Carving Attributed Dump Sets.
   T. van Deursen, S. Mauw, Sasa Radomirovic
9. SHELLOS: Enabling Fast Detection and Forensic Analysis of Code Injection Attacks.
   K.Z. Snow, S. Krishnan, F. Monrose, N. Provos
10. MACE: Model-inference-Assisted Concolic Exploration for Protocol and Vulnerability Discovery.
    C.Y. Cho, D. Babic, P. Poosankam, K.Z. Chen, E. XueJun Wu, D. Song
11. Static Detection of Access Control Vulnerabilities in Web Applications.
    F. Sun, L. Xu, Z. Su
12. ADsafety: Type-Based Verification of JavaScript Sandboxing.
    J. Gibbs Politz, S.A. Eliopoulos, A. Guha, S. Krishnamurthi
13. Measuring Pay-per-Install: The Commoditization of Malware Distribution.
    (Outstanding Paper Award) J. Caballero, C. Grier, C. Kreibich, V. Paxson
14. Dirty Jobs: The Role of Freelance Labor in Web Service Abuse.
    M. Motoyama, D. McCoy, K. Levchenko, S. Savage, G.M. Voelker
15. Show Me the Money: Characterizing Spam-advertised Revenue.
    C. Kanich, N. Weaver, D. McCoy, T. Halvorson, C. Kreibich, K. Levchenko, V. Paxson, G.M. Voelker, S. Savage
16. Secure In-Band Wireless Pairing.
    S. Gollakota, N. Ahmed, N. Zeldovich, D. Katabi
17. TRESOR Runs Encryption Securely Outside RAM.
    T. Muller, F.C. Freiling; A. Dewald
18. Bubble Trouble: Off-Line De-Anonymization of Bubble Forms.
    J.A. Calandrino, W. Clarkson, E.W. Felten
19. Measuring and Analyzing Search-Redirection Attacks in the Illicit Online Prescription Drug Trade.
    N. Leontiadis, T. Moore, N. Christin
20. deSEO: Combating Search-Result Poisoning.
    J.P. John, F. Yu, Y. Xie, A. Krishnamurthy, M. Abadi
21. A Study of Android Application Security.
    W. Enck, D. Octeau, P. McDaniel, S. Chaudhuri
22. Permission Re-Delegation: Attacks and Defenses.
    A. Porter Felt, H.J. Wang, A. Moshchuk, S. Hanna, E. Chin
23. QUIRE: Lightweight Provenance for Smart Phone Operating Systems.
    M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu, D.S. Wallach
24. SMS of Death: From Analyzing to Attacking Mobile Phones on a Large Scale.
    C. Mulliner, N. Golde, J.-P. Seifert
25. Q: Exploit Hardening Made Easy.
    E.J. Schwartz, T. Avgerinos, D. Brumley
26. Cloaking Malware with the Trusted Platform Module.
    A.M. Dunn, O.S. Hofmann, B. Waters, E. Witchel
27. Detecting Malware Domains at the Upper DNS Hierarchy.
    M. Antonakakis, R. Perdisci, W. Lee, N. Vasiloglou II, D. Dagon
28. BOTMAGNIFIER: Locating Spambots on the Internet.
    G. Stringhini, T. Holz, B. Stone-Gross, C. Kruegel, G. Vigna
29. JACKSTRAWS: Picking Command and Control Connections from Bot Traffic.
    G. Jacob, R. Hund, C. Kruegel, T. Holz
30. Telex: Anticensorship in the Network Infrastructure.
    E. Wustrow, S. Wolchok, I. Goldberg, J. Alex Halderman
31. PIR-Tor: Scalable Anonymous Communication Using Private Information Retrieval.
    P. Mittal, F. Olumofin, C. Troncoso, N. Borisov, I. Goldberg

32. The Phantom Tollbooth: Privacy-Preserving Electronic Toll Collection in the Presence of Driver Collusion.
    S. Meiklejohn, K. Mowery, S. Checkoway, H. Shacham
33. Differential Privacy Under Fire.
    A. Haeberlen, B.C. Pierce, A. Narayan
34. Outsourcing the Decryption of ABE Ciphertexts.
    M. Green, S. Hohenberger, B. Waters
35. Faster Secure Two-Party Computation Using Garbled Circuits.
    Y. Huang, D. Evans, J. Katz, L. Malka

(Invited talk, among others; slides online): The (Decentralized) SSL Observatory.
P. Eckersley, J. Burns

(Panel, among others; video online): SSL/TLS Certificates: Threat or Menace?
Eric Rescorla (moderator), A. Langley (Google), B. Smith (Mozilla), S. Schultze (Princeton U.), S. Kent (BBN)

ACM CCS 2011

(Keynote address): Reflections on the Evolution of Internet Threats: The Growing Imperative for a Cyber Secure Society.
Farnam Jahanian

1. VIPER: Verifying the Integrity of PERpherals' Firmware.
   Y. Li, Jonathan M. McCune, Adrian Perrig
2. Unicorn: Two-Factor Attestation for Data Security.
   M. Mannan, B. Heyn Kim, A. Ganjali, D. Lie
3. Combining Control-Flow Integrity and Static Analysis for Efficient and Validated Data Sandboxing.
   B. Zeng, G. Tan, G. Morrisett
4. Composition Theorems Without Pre-Established Session Identifiers.
   R. Kusters, M. Tuengerthal
5. Composability of Bellare-Rogaway Key Exchange Protocols.
   C. Brzuska, M. Fischlin, B. Warinschi, S.C. Williams
6. A Composable Computational Soundness Notion.
   V. Cortier, B. Warinschi,
7. On the Requirements for Successful GPS Spoofing Attacks.
   N. Ole Tippenhauer, C. Popper, K.B. Rasmussen, S. Capkun
8. Protecting Consumer Privacy from Electric Load Monitoring.
   S. McLaughlin, P. McDaniel, W. Aiello
9. PaperSpeckle: Microscopic Fingerprinting of Paper.
   A. Sharma, L. Subramanian, E. Brewer
10. On the Vulnerability of FPGA Bitstream Encryption Against Power Analysis Attacks.
    A. Moradi, A. Barenghi, T. Kasper, C. Paar
11. Text-based CAPTCHA Strengths and Weaknesses.
    E. Bursztein, M. Martin, J.C. Mitchell
12. An Efficient User Verification System via Mouse Movements.
    N. Zheng, A. Paloski, H. Wang
13. Policy Auditing over Incomplete Logs: Theory, Implementation and Applications.
    D. Garg, L. Jia, A. Datta
14. Automatic Error Finding in Access-Control Policies.
    K. Jayaraman, V. Ganesh, M. Tripunitara, M. Rinard, S. Chapin
15. Trust-based Anonymous Communication: Adversary Models and Routing Algorithms.
    A. Johnson, P. Syverson, R. Dingledine, N. Mathewson
16. Cirripede: Circumvention Infrastructure Using Router Redirection with Plausible Deniability.
    A. Houmansadr, G.T.K. Nguyen, M. Caesar, N. Borisov
17. Forensic Investigation of the OneSwarm Anonymous Filesharing System.
    S. Prusty, B.N. Levine, M. Liberatore
18. Stealthy Traffic Analysis of Low-Latency Anonymous Communication Using Throughput Fingerprinting.
    P. Mittal, A. Khurshid, J. Juen, M. Caesar, N. Borisov
19. App Isolation: Get the Security of Multiple Browsers with Just One.
    E.Y. Chen, J. Bau, C. Reis, A. Barth, C. Jackson
20. Crouching Tiger - Hidden Payload: Security Risks of Scalable Vectors Graphics.
    M. Heiderich, T. Frosch, M. Jensen, T. Holz
21. Fear the EAR: Discovering and Mitigating Execution After Redirect Vulnerabilities.
    A. Doupe, B. Boe, C. Kruegel, G. Vigna
22. Automated Black-Box Detection of Side-Channel Vulnerabilities in Web Applications.
    P. Chapman, D. Evans
23. Deobfuscation of Virtualization-Obfuscated Software.
    K. Coogan, G. Lu, S. Debray
24. The Power of Procrastination: Detection and Mitigation of Execution-Stalling Malicious Code.
    C. Kolbitsch, E. Kirda, C. Kruegel
25. MIDeA: A Multi-Parallel Intrusion Detection Architecture.
    G. Vasiliadis, M. Polychronakis, S. Ioannidis
26. BitShred: Feature Hashing Malware for Scalable Triage and Semantic Analysis.
    J. Jang, D. Brumley, S. Venkataraman
27. Trace Equivalence Decision: Negative Tests and Non-determinism.
    V. Cheval, H. Comon-Lundh, S. Delaune
28. Extracting and Verifying Cryptographic Models from C Protocol Code by Symbolic Execution.
    M. Aizatulin, A. D. Gordon, J. Jurjens
29. Modular Code-Based Cryptographic Verification.
    C. Fournet, M. Kohlweiss, P.-Y. Strub
30. Information-Flow Types for Homomorphic Encryptions.
    C.Fournet, J. Planul, T. Rezk

31. Process Out-Grafting: An Efficient "Out-of-VM" Approach for Fine-Grained Process Execution Monitoring.
    D. Srinivasan, Z. Wang, X. Jiang, D. Xu
32. SICE: A Hardware-Level Strongly Isolated Computing Environment for x86 Multi-Core Platforms.
    A.M. Azab, P. Ning, X. Zhang
33. AmazonIA: When Elasticity Snaps Back.
    S. Bugiel, S. Nurnberger, T. Poppelmann, A.-R. Sadeghi, T. Schneider
34. Eliminating the Hypervisor Attack Surface for a More Secure Cloud.
    J. Szefer, E. Keller, R.B. Lee, J. Rexford
35. How to Break XML Encryption.
    T. Jager, J. Somorovsky
36. Ciphers That Securely Encipher Their Own Keys.
    M. Bellare, D. Cash, S. Keelveedhi
37. Password-Protected Secret Sharing.
    A. Bagherzandi, S. Jarecki, N. Saxena, Y. Lu
38. Practical Delegation of Computation Using Multiple Servers.
    R. Canetti, B. Riva, G.N. Rothblum
39. Fashion Crimes: Trending-Term Exploitation on the Web.
    T. Moore, N. Leontiadis, N. Christin
40. SURF: Detecting and Measuring Search Poisoning.
    L. Lu, R. Perdisci, W. Lee
41. Cloak and Dagger: Dynamics of Web Search Cloaking.
    D.Y. Wang, S. Savage, G.M. Voelker
42. Proofs of Ownership in Remote Storage Systems.
    S. Halevi, D. Harnik, B. Pinkas, A. Shulman-Peleg
43. How to Tell if Your Cloud Files Are Vulnerable to Drive Crashes.
    K.D. Bowers, M. van Dijk, A. Juels, A. Oprea, R.L. Rivest
44. Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds.
    K. Zhang, X. Zhou, Y. Chen, X. Wang, Y. Ruan
45. iSpy: Automatic Reconstruction of Typed Input from Compromising Reflections.
    R. Raguram, A.M. White, D. Goswami, F. Monrose, J.-M. Frahm
46. Televisions, Video Privacy, and Powerline Electromagnetic Interference.
    M. Enev, S. Gupta, T. Kohno, S.N. Patel
47. (sp)iPhone: Decoding Vibrations from Nearby Keyboards Using Mobile Phone Accelerometers.
    P. Marquardt, A. Verma, H. Carter, P. Traynor
48. Predictive Mitigation of Timing Channels in Interactive Systems.
    D. Zhang, A. Askarov, A.C. Myers
49. WAPTEC: Whitebox Analysis of Web Applications for Parameter Tampering Exploit Construction.
    P. Bisht, T. Hinrichs, N. Skrupsky, V.N. Venkatakrishnan
50. Context-Sensitive Auto-Sanitization in Web Templating Languages Using Type Qualifiers.
    M. Samuel, P. Saxena, D. Song,
51. SCRIPTGARD: Automatic Context-Sensitive Sanitization for Large-Scale Legacy Web Applications.
    P. Saxena, D. Molnar, B. Livshits
52. Fortifying Web-Based Applications Automatically.
    S. Tang, N. Dautenhahn, S.T. King
53. Android Permissions Demystified.
    A. Porter Felt, E. Chin, S. Hanna, D. Song, D. Wagner
54. "These Aren't the Droids You're Looking For": Retrofitting Android to Protect Data from Imperious Applications.
    P. Hornyack, S. Han, J. Jung, S. Schechter, D. Wetherall
55. Privacy and Accountability for Location-based Aggregate Statistics.
    R. Ada Popa, A. J. Blumberg, H. Balakrishnan, F.H. Li
56. Auctions in Do-Not-Track Compliant Internet Advertising.
    A. Reznichenko, S. Guha, P. Francis
57. Practical PIR for Electronic Commerce.
    R. Henry, F. Olumofin, I. Goldberg
58. Countering GATTACA: Efficient and Secure Testing of Fully-Sequenced Human Genomes.
    P. Baldi, R. Baronio, E. De Cristofaro, P. Gasti, G. Tsudik
59. Automatically Optimizing Secure Computation.
    F. Kerschbaum
60. VMCrypt - Modular Software Architecture for Scalable Secure Computation.
    L. Malka

(Keynote address): Cryptographic Primitives for Building Secure and Privacy Respecting Protocols.
J. Camenisch