

Topics

- Topic 1: RFID Security
- Topic 2: Captcha
- Topic 3: Untrusted Storage
- Topic 4: SmartPhone Security
- Topic 5: Attacks on SmartPhone
- Topic 6: Password Protection
- Topic 7: Distributed Denial of Service Attacks
- Topic 8: Sybil Attacks
- Topic 9: Behavioural Biometrics
- Topic 10: VoIP Security
- Topic 11: Secure Content Delivery
- Topic 12: Anonymous Communications
- Topic 13: Keyloggers Detection
- Topic 14: Anonymity in WSN
- Topic 15: Botnet Detection
- Topic 16: Trusted HW
- Topic 17: Security of RFID ePassports
- Topic 18: Node Replication Attack in WSN
- Topic 19: Secure Data Aggregation in WSN
- Topic 20: Privacy issues in Social Networks
- Topic 21: Google Android smartphone security
- Topic 22: Electronic Voting
- Topic 23: P2P BotNet Detection
- Topic 24: Taint Mechanisms
- Topic 25: Browser Security
- Topic 26: Privacy of Location Based Services
- Topic 27: Named Data Networking Security
- Topic 28: Named Data Networking Privacy
- Topic 29: Cloud Security
- Topic 30: Anonymity in Wireless Network
- Topic 31: Smartphone User Profiling
- Topic 32: SSL security issues in Android
- Topic 33: Circumvent censorship

Topic 1: RFID Security

Primary:

- M.R. Rieback, G.N. Gaydadjiev, B. Crispo, R.F.H. Hofman and A.S. Tanenbaum, [A Platform for RFID Security and Privacy Administration](#), Proceedings of the 20th USENIX/SAGE Large Installation System Administration Conference (LISA 2006).

Secondary:

- A. Juels, P. Syverson, D. Bailey, [High-Power Proxies for Enhancing RFID Privacy and Utility](#), Privacy Enhancing Technologies (PET) Workshop, pp. 210-226. 2005.
- G. P. Hancke, [Practical Attacks on Proximity Identification Systems](#), Proceedings of the 2006 IEEE Symposium on Security and Privacy
- A. Juels, [RFID Security and Privacy: A Research Survey](#), IEEE Journal on Selected Areas in Communications, Vol. 24, No. 2, February 2006.

Topic 2: Captcha

Primary:

- J. Yan, A. Salah El Ahmad, [A Low-cost Attack on a Microsoft CAPTCHA](#), ACM CCS 2008.

Secondary:

- Marti Motoyama, Kirill Levchenko, Chris Kanich, Damon McCoy, Geoffrey M. Voelker, and Stefan Savage [Re: CAPTCHAs. Understanding CAPTCHA-Solving Services in an Economic Context](#), Proceedings of Usenix Security 2010.
- J Yan and Ahmad El Ahmad., [Breaking Visual CAPTCHAs with Naive Pattern Recognition Algorithms](#), Proceedings of ACSAC 2007 .
- H. S. Baird, T. Riopka, [ScatterType: a Reading CAPTCHA Resistant to Segmentation Attack](#), Proceedings of SPIE/IS&T Conf. on Document Recognition and Retrieval XII (DR&R2005). .

Topic 3: Untrusted Storage

Primary:

- P. Mahajan, S. Setty, S. Lee, A. Clement, L. Alvisi, M. Dahlin, and M. Walfish [Depot: Cloud Storage with Minimal Trust](#), In the proceedings of USENIX Symposium on Operating Systems Design and Implementation (OSDI 2010).

Secondary:

- Geron, E.; Wool, A, [CRUST: Cryptographic Remote Untrusted Storage without Public Keys](#), In the proceedings of The Fourth International IEEE Security in Storage Workshop, 2007.
- Eu-Jin Goh, H. Shacham, N. Modadugu, D. Boneh, [SiRiUS: Securing Remote Untrusted Storage](#), In proceedings of the Internet Society (ISOC) Network and Distributed Systems Security (NDSS) Symposium 2003.

Topic 4: SmartPhone Security

Primary:

- S. Heuser, A. Nadkarni, W. Enck, A. Sadeghi, [ASM: A Programmable Interface for Extending Android Security](#), Proc. of the 23rd USENIX Security Symposium.

Secondary:

- G. Russello, M. Conti, B. Crispo, and E. Fernandes, [MOSES: Supporting Operation Modes on Smartphones](#), ACM SACMAT 2012.
- M. Dietz, S. Shekhar, Y. Pisetsky, A. Shu and Dan S. Wallach, [Quire: Lightweight Provenance for Smart Phone Operating Systems](#), Proceedings of the 20th USENIX Security Symposium, 2011
- P. Hornyack, S. Han, J. Jung, S. Schechter, and D. Wetherall, ["These Aren't the Droids You're Looking For": Retrofitting Android to Protect Data from Imperious Applications](#),

Proc. of the 18th ACM Conference on Computer and Communications Security (ACM CCS 2011)

Topic 5: Attacks on SmartPhone

Primary:

- C. Lin¹, H. Li¹, X. Zhou², X. Wang², [Screenmilk: How to Milk Your Android Screen for Secrets](#), Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS), 2014.

Secondary:

- K. Mowery, S. Meiklejohn, S. Savage, [Heat of the moment: characterizing the efficacy of thermal camera-based attacks](#), WOOT'11 Proceedings of the 5th USENIX conference on Offensive technologies, 2011.
- Li. Cai, H. Chen "[TouchLogger: Inferring Keystrokes On Touch Screen From Smartphone Motion](#)", In Proceedings of HotSec '11, 2011

Topic 6: Password Protection

Primary:

- S. Komanduri, R. Shay, and L. Cranor, C. Herley and S. Schechter, [Telepathwords: preventing weak passwords by reading users'™ minds](#), Proceedings of the 23rd Conference on USENIX Security Symposium 2014.

Secondary:

- J.A Halderman, B. Waters, E.W. Felten, [A Convenient Method for Securely Managing Passwords](#), Proceedings of the 14th International Conference on World Wide Web 2005, May 2005, Chiba, Japan, pp. 471-479.
- B. Ross, C. Jackson, N. Miyake, D. Boneh, J. C Mitchell, [Stronger Password Authentication Using Browser Extensions](#), Proceeding of 14th USENIX Security Symposium 2005, Vol. 14, Baltimore, MD USA, 31 July - 5 August, 2005, pp. 17-31.
- X. de Carnavalet and M. Mannan, [From Very Weak to Very Strong: Analyzing Password-Strength Meters](#), Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS), 2014.
- S. Chiasson, P.C. van Oorschot, R. Biddle, [A Usability Study and Critique of Two Password Managers](#), Proceedings of the 15th Conference on USENIX Security Symposium 2006, Vol. 15, August 2006, Vancouver Canada, pp. 1-16.
- J. Thorpe, P. van Oorschot, [Graphical Dictionaries and the Memorable Space of Graphical Passwords](#), Proceedings of 13th USENIX Security Symposium 2004, San Diego, CA, USA, 9-13 August, 2004, pp. 135-140.

Topic 7: Distributed Denial of Service Attacks

Primary:

- C. Rossow, [Amplification Hell: Revisiting Network Protocols for DDoS Abuse](#), Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS), 2014.

Secondary:

- D. Moore, G.M. Voelker, S. Savage, [Inferring Internet Denial-of-Service Activity](#), Proceedings of the 10th USENIX Security Symposium 2001, Washington, DC, USA, August, 2001, pp. 115-139.

- A. Yaar, A. Perrig, D. Song, [Pi: A Path Identification Mechanism to Defend against DDoS Attacks](#), Proceedings of the 2003 IEEE Symposium on Security and Privacy, Oakland, CA, USA, May 2003, pp. 93-107.
- J. Mirkovic, P. Reiher, [D-WARD: A Source-End Defense Against Flooding Denial-of-Service Attacks](#), IEEE Transactions on Dependable and Secure Computing, Vol. 2, No. 3, September 2005, pp. 216-232.
- J.Mirkovic, P.Reiher, S.Fahmy, R.Thomas, A.Hussein, S.Schwab, C.Ko, "[Measuring Denial-of-Service](#)", Proceedings of 2006 Quality of Protection Workshop, October 2006.
- D. Champagne, R. B. Lee, [Scope of DDoS Countermeasures: Taxonomy of Proposed Solutions and Design Goals for Real-World Deployment](#), Proceedings of the 8th International Symposium on Systems and Information Security (SSI'2006), Sao Paulo, Brazil November 2006.
- A. Yaar, A. Perrig, D. Song, [SIFF: A Stateless Internet Flow Filter to Mitigate DDoS Flooding Attacks](#), Proceedings of the IEEE Security and Privacy Symposium, 2004.

Topic 8: Sybil Attacks

Primary:

- H. Yu, M. Kaminsky, P.B. Gibbons, A. Flaxman, [SybilGuard: Defending Against Sybil Attacks via Social Networks](#), In Proceedings of the ACM SIGCOMM Conference on Computer Communications (SIGCOMM 2006).

Secondary:

- H. Yu, M. Kaminsky, P.B. Gibbons, F. Xiao, [SybilLimit: A Near-Optimal Social Network Defense against Sybil Attacks](#), 2008 IEEE Symposium on Security and Privacy, 2008.
- S. D. Kamvar, M. T. Schlosser, H.Garcia Molina [The EigenTrust Algorithm for Reputation Management in P2P Networks](#), Proceedings of the International World Wide Web Conference (WWW 2003) .

Additional Reading:

- J. R. Douceur, [The Sybil Attack](#), First International Workshop on Peer-to-Peer Systems 2002.

Topic 9: Behavioural Biometrics

Primary:

- M.Conti, I. Zuchia-Zlatea, and B. Crispo, [Mind How You Answer Me! \(Transparently Authenticating the User of a Smartphone when Answering or Placing a Call\)](#), Proceedings of the Sixth ACM Symposium on Information, Computer and Communications Security (ASIACCS 2011).

Secondary:

- Derawi, M.O.; Nickel, C.; Bours, P.; Busch, C. [Unobtrusive User-Authentication on Mobile Phones using Biometric Gait Recognition](#) , in the proceedings of the Sixth International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2010.
- P. Yan and K. W. Bowyer, [Biometric Recognition Using 3D Ear Shape](#), IEEE TRANSACTIONS ON PATTERN ANALYSIS AND MACHINE INTELLIGENCE, VOL. 29, NO. 8, AUGUST 2007.
- S. Zahid, M. Shahzad, S. A. Khayam, M. Farooq, [Keystroke-based User Identification on](#)

[Smart Phones](#), Proceedings of Recent Advances in Intrusion Detection (RAID 2009).

Topic 10: VoIP Security

Primary:

- H. Sengar [VoIP Fraud: Identifying a Wolf in Sheep's Clothing](#), Proceeding CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.

Secondary:

- D.C. Sicker, T. Lookabaugh [VoIP Security: Not an Afterthought](#), Queue archive Volume 2 , Issue 6 (September 2004)
- C.V. Wright, L. Ballard, S.E. Coull, F. Monrose, and G.M. Masson, [Spot Me if You Can: Uncovering Spoken Phrases in Encrypted VoIP Conversations](#), In Proceedings of the 2008 IEEE Symposium on Security and Privacy, 2008.
- X. Wang, S. Chen, S. Jajodia [Tracking Anonymous PeertoPeer VoIP Calls on the Internet](#), Proceedings of the 12th ACM Conference on Computer Communications Security (CCS 2005).

Topic 11: Secure Content Delivery

Primary:

- N. Michalakis R. Soule, R. Grimm, [Ensuring Content Integrity for Untrusted Peer-to-Peer Content Distribution Networks](#), 4th USENIX Symposium on Networked Systems Design & Implementation (NSDI 2007).

Secondary:

- B.C Popescu, B. Crispo, A. Tanenanbaum [Secure data Replication over Untrusted Hosts](#), Proceedings of the 5th Usenix UNIX Security Symposium, Vol. 5, Salt Lake City, Utah, USA, June 1995, pp. 199-208.
- K. Fu, M.F. Kaashoek, D. Mazieres, [Fast and secure distributed read-only filesystem](#), Proceedings of the 4th Symposium on Operating Systems Design and Implementation OSDI 2000
- M. Castro, B. Liskov, [Practical Byzantine Fault Tolerance](#), Proceedings of the 3rd Symposium on Operating Systems Design and Implementation OSDI 1999.

Topic 12: Anonymous Communications

Primary:

- R. Jansen, F. Tschorsch, A. Johnson, B. Scheuermann, [The Sniper Attack: Anonymously Deanonymizing and Disabling the Tor Network](#), Proceedings of the 21th Annual Network and Distributed System Security Symposium (NDSS), 2014.

Secondary:

- S. J. Murdoch, G. Danezis, [Low-Cost Traffic Analysis of Tor](#), Proceedings of the IEEE Symposium on Security and Privacy, 2005
- R. Dingledine, N. Mathewson, P. Syverson, [Tor: The Second-Generation Onion Router](#), Proceedings of the 13th USENIX Security Symposium (August 2004)
- Nathan S. Evans, Roger Dingledine, and Christian Grothoff., [A Practical Congestion Attack on Tor Using Long Paths](#), Proceedings of the 18th USENIX Security Symposium 2009
- M. Backes, A. Kate, S. Meiser and E. Mohammadi, [\(Nothing else\) MATor\(s\): Monitoring](#)

[the Anonymity of Tor's Path Selection](#), Proceeding CCS '14 Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security.

Topic 13: Keyloggers Detection

Primary:

- S Ortolani, C Giuffrida and B. Crispo [Bait your hook: a novel detection technique for keyloggers](#) , Proceedings of Recent Advances in Intrusion Detection (RAID 2010)

Secondary:

- S Ortolani, C Giuffrida and B. Crispo, [KLIMAX: Profiling Memory Write Patterns to Detect Keystroke-Harvesting Malware](#) , Proceedings of Recent Advances in Intrusion Detection (RAID 2011)
- D. Le, C. Yue, T. Smart, H. Wang: , [Detecting kernel level keyloggers through dynamic taint analysis](#), Technical Report WM-CS-2008-05, College William and Mary, 2008
- K. Nasaka, T. Takami, T. Yamamoto, and M. Nishigaki, [A Keystroke Logger Detection Using Keyboard-Input-Related API Monitoring](#) , Proceedings of the 14th International Conference on Network-Based Information Systems, 2009

Topic 14: Anonymity in WSN

Primary:

- Yang et al. [Towards event source unobservability with minimum network traffic in sensor networks](#), Proceedings of the first ACM conference on Wireless network security (2008) pp. 77-88

Secondary:

- S. Ortolani, M. Conti, B. Crispo, and R. Di Pietro, [Events Privacy in WSNs: a New Model and its Application](#), Proceedings of the Twelfth IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WOWMOM 2011).
- Shao et al., [Towards statistically strong source anonymity for sensor networks](#), Proceedings of IEEE INFOCOM 2008. The 27th Conference on Computer Communications (2008) pp. 51-55
- Hoh and Gruteser. [Protecting location privacy through path confusion](#), Proceedings of the Security and Privacy for Emerging Areas in Communications Networks, 2005. SecureComm 2005. pp. 194-205 ,

Topic 15: Botnet Detection

Primary:

- G. Gu, J. Zhang, and W. Lee., [BotSniffer: Detecting botnet command and control channels in network traffic](#), Proceedings of the 15th Annual Network and Distributed System Security Symposium (NDSS\9208), 2008.

Secondary:

- Guofei Gu, Roberto Perdisci, Junjie Zhang and Wenke Lee, [BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection](#), Proceedings of 17th Usenix Security Symposium. (2008)
- G. Gu, P. Porras, V. Yegneswaran, M. Fong, and W. Lee. . [BotHunter: Detecting malware infection through ids-driven dialog correlation](#), In Proceedings of the 16th USENIX Security Symposium (Security\9207), 2007.
- A. Karasaridis, B. Rexroad, and D. Hoeflin. . [Widescale botnet detection and](#)

[characterization](#), Proceedings of USENIX HotBots\9207, 2007

Topic 16: Trusted HW

Primary:

- Drimer, S. Murdoch, S.J. Anderson, R., [Thinking Inside the Box: System-Level Failures of Tamper Proofing](#), Proceedings of the IEEE Symposium on Security and Privacy, 2008.
- Ross Anderson, Markus Kuhn , [Tamper Resistance --- a Cautionary Note](#), In Proceedings of the Second Usenix Workshop on Electronic Commerce, 1996.
- Oliver K\F6mmerling, Markus G. Kuhn, [Design principles for tamper-resistant smartcard processors](#), Proceedings of the USENIX Workshop on Smartcard Technology 1999
- Ross J. Anderson, Markus G. Kuhn., [Low Cost Attacks on Tamper Resistant Devices](#), Proceedings of Security Protocols Workshop 1997: 125-136

Secondary:

Topic 17: Security of RFID ePassports

Primary:

- Karl Koscher, Ari Juels, Tadayoshi Kohno and Vjekoslav Brajkovic, [EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond](#), 2008.
- Gildas Avoine, Kassem Kalach and Jean-Jacques Quisquater., ["ePassport: Securing International Contacts with Contactless Chips."](#), In Proceedings of Financial Cryptography Conference, 2008.
- Rishab Nithyanand., [A survey on the Evolution of Cryptographic Protocols in Electronic Passports](#), IACR ePrint 2009
- Eleni Kosta, Martin Meints, Marit Hensen, and Mark Gasson. [An analysis of security and privacy issues relating to RFID enabled ePassports](#), Proceedings of IFIP SEC 2007

Secondary:

Topic 18: Node Replication Attack in WSN

Primary:

- Bryan Parno, Adrian Perrig, Virgil Gligor, [Distributed Detection of Node Replication Attacks in Sensor Networks](#), Proceedings of the 2005 IEEE Symposium on Security and Privacy, p.49-63.

Secondary:

- H. Choi, S. Zhu, and T. La Porta. [SET: Detecting Node Clones in Sensor Networks](#), In Proceedings of SecureComm, Sep. 2007.
- Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei. [Distributed Detection of Clone Attacks in Wireless Sensor Networks](#), In IEEE Transactions on Dependable and Secure Computing (TDSC), Vol. 99, 2010, to appear.

Topic 19: Secure Data Aggregation in WSN

Primary:

- Haowen Chan , Adrian Perrig, Dawn Song, [Secure hierarchical in-network aggregation in sensor networks](#), Proceedings of the 13th ACM conference on Computer and communications security, 2006,

Secondary:

- Keith B. Frikken, Joseph A. Dougherty. [An efficient integrity-preserving scheme for](#)

[hierarchical sensor aggregation](#), Proceedings of the first ACM conference on Wireless network security, 2008.

- Sankardas Roy, Mauro Conti, Sanjeev Setia, Sushil Jajodia, [Secure Median Computation in Wireless Sensor Networks](#), Elsevier Ad Hoc Networks, 2009.
- Sankardas Roy, Mauro Conti, Sanjeev Setia, Sushil Jajodia, [Secure Data Aggregation in Wireless Sensor Networks](#), IEEE Transactions on Information Forensics & Security, 7(3): 1040-1052, 2012.

Topic 20: Privacy issues in Social Networks

Primary:

- M. Conti, A. Hasani, and B. Crispo [Virtual Private Social Networks and a Facebook Implementation](#), ACM Transactions on the Web, 2013.

Secondary:

- Wanying Luo, Qi Xie, and Urs Hengartner [FaceCloak: An architecture for user privacy on social networking sites](#), Proceedings of the 2009 international conference on computational science and engineering, 2009.
- Saikat Guha, Kevin Tang, and Paul Francis, [NOYB: Privacy in online social networks](#), Proceedings of the first USENIX Workshop on Online Social Networks, 2008.
- Randy Baden, Adam Bender, Neil Spring, Bobby Bhattacharjee, Daniel Starin, and Starin Consulting, [Persona: an online social network with user-defined privacy](#), Proceedings of the ACM SIGCOMM 2009 conference on Data communication, 2009.
- M. Conti, R. Poovendran, M. Secchiero, [FakeBook: Detecting Fake Profiles in On Line Social Networks](#), ACM/IEEE CSOSN 2012.
- F. Beato, I. Ion, S. Capkun, M. Langheinrich, and B. Preneel, [For Some Eyes Only: Protecting Online Information Sharing](#), ACM CODASPY 2012.

Topic 21: Google Android smartphone security

Primary:

- William Enck, Machigar Ongtang, and Patrick McDaniel, [On Lightweight Mobile Phone App Certification](#), Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS), 2009

Secondary:

- Machigar Ongtang, Stephen McLaughlin, William Enck, and Patrick McDaniel, [Semantically Rich Application-Centric Security in Android](#), Proceedings of the 25th Annual Computer Security Applications Conference (ACSAC), 2009.
- William Enck, Machigar Ongtang, and Patrick McDaniel, [Understanding Android Security](#), IEEE Security & Privacy Magazine, 7(1):50--57, January/February, 2009.
- Mauro Conti, Bruno Crispo, Earlene Fernandes, Yury Zhauniarovich [CREPE: a System for Enforcing Fine-Grained Context-Related Policies on Android](#), IEEE Transactions on Information Forensics & Security 2012.

Topic 22: Electronic Voting

Primary:

- D. Balzarotti, G. Banks, M. Cova, V. Felmetzger, R. Kemmerer, W. Robertson, F. Valeur, and G. Vigna, [An Experience in Testing the Security of Real-world Electronic Voting Systems](#), IEEE Transactions on Software Engineering, no. 36(4) July/August

2010.

Secondary:

- Nathanael Paul, Andrew Tanenbaum, [The Design of a Trustworthy Voting System](#), Computer Security Applications Conference, ACSAC '09, p. 507 - 517, 2009.
- A. Feldman, J. Halderman, and E. Felten, [Security Analysis of the Diebold AccuVote-TS Voting Machine](#), USENIX Workshop on Accurate Electronic Voting Technology (EVT '07), p.2, 2007.
- Daniel R. Sandler, Kyle Derr, Dan S. Wallach, [VoteBox: A tamper-evident, verifiable electronic voting system](#), USENIX Security Symposium (Security '08), 2008.

Topic 23: P2P BotNet Detection

Primary:

- Shishir Nagaraja, Prateek Mittal, Chi-Yao Hong, Matthew Caesar, and Nikita Borisov [BotGrep: Finding P2P Bots with Structured Graph Analysis](#), Usenix Security 2010.

Secondary:

- Su Chang and Thomas E. Daniels [P2P botnet detection using behavior clustering and statistical tests](#), Proceedings of the 2nd ACM workshop on Security and artificial intelligence (2009).
- ME1rk Jelasity and Vilmos Bilicki, [Towards Automated Detection of Peer-to-Peer Botnets: On the Limits of Local Approaches](#), Usenix LEET 2009.
- Jian Kang, Jun-Yao Zhang, Qiang Li, Zhuo Li [Detecting New P2P Botnet with Multi-chart CUSUM](#), 2009 International Conference on Networks Security, Wireless Communications and Trusted Computing.

Topic 24: Taint Mechanisms

Primary:

- Edward J. Schwartz, Thanassis Avgerinos, David Brumley, [All You Ever Wanted to Know About Dynamic Taint Analysis and Forward Symbolic Execution \(but might have been afraid to ask\)](#), IEEE Security & Privacy 2010.

Secondary:

- Bruno P.S. Rocha, Sruthi Bandhakavi, Jerry den Hartog, William H. Winsborough, Sandro Etalle, [Towards Static Flow-based Declassification for Legacy and Untrusted Programs](#), IEEE Security & Privacy 2010.
- W. Enck, P. Gilbert, B. Chun, L.P. Cox, J. Jung, P. McDaniel, A. Sheth, [TaintDroid: An Information-Flow Tracking System for Realtime Privacy Monitoring on Smartphones](#), OSDI 2010.
- Asia Slowinska, Herbert Bos, [Pointless tainting?: evaluating the practicality of pointer tainting](#), EuroSys '09.

Topic 25: Browser Security

Primary:

- A. Kapravelos, C. Grier, N. Chachra, C. Kruegel, G. Vigna, V. Paxson [Hulk: Eliciting Malicious Behavior in Browser Extensions](#), USENIX Security Symposium (Security '14), 2014

Secondary:

- Philippe De Ryck, Lieven Desmet, Thomas Heyman, Frank Piessens, Wouter

JoosenCsFire: [Transparent Client-Side Mitigation of Malicious Cross-Domain Requests](#) ESSOS 2010.

- T. Oda, G. Wurster, P. van Oorschot, and A. Somayaji [SOMA: mutual approval for included content in web pages](#) ACM conference on Computer and communications security 2008.
- Adam Barth, Collin Jackson, and John C. Mitchell [Robust Defenses for Cross-Site Request Forgery](#) ACM Conference on Computer and Communications Security 2008

Topic 26: Privacy of Location Based Services

Primary:

- M. L. Damiani, E. Bertino, and C. Silvestri, [The probe framework for the personalized cloaking of private locations](#), Transactions on Data Privacy, pages 123-148, 2010.
- Secondary:
- Toby Xu and Ying Cai, [Feeling-based location privacy protection for location-based services](#), In CCS '09, 2009.
 - G. Ghinita, P. Kalnis, A. Khoshgozaran, C. Shahabi, and K. Tan, [Private queries in location based services: anonymizers are not necessary](#), In SIGMOD '08, pages 121-132, 2008.
 - Luciana Marconi, Roberto Di Pietro, Bruno Crispo, and Mauro Conti, [Time Warp: how time affects privacy in LBSs](#), In Proceedings of the twelfth International Conference on Information and Communications Security (ICICS), pages to appear, 2010.

Topic 27: Named Data Networking Security

Primary:

- C. Ghali, G. Tsudik, E. Uzun, [Network-Layer Trust in Named-Data Networking](#) , ACM Computer Communication Review.

Secondary:

- C. Ghali, G. Tsudik, E. Uzun, [Needle in a Haystack: Mitigating Content Poisoning in Named-Data Networking](#) , NDSS Workshop on Security of Emerging Networking Technologies, 2014.
- P. Mahadevan, E. Uzun, S. Sevilla, [CCN key resolution service](#) , Proceedings of the 1st international conference on Information-centric networking (ICN 2014).
- M. Conti, P. Gasti, M. Teoli, [A Lightweight Mechanism for Detection of Cache Pollution Attacks in Named Data Networking](#) , In (Elsevier) Computer Networks, 2013.

Topic 28: Named Data Networking Privacy

Primary:

- S. DiBenedetto, P. Gasti, G. Tsudik, and E. Unzun, [ANDaNA: Anonymous named data networking application](#) , In NDSS 2012.

Secondary:

- A. Chaabane, E. De Cristofaro, M. Kafaar, E. Uzun, [Privacy in Content-Oriented Networking: Threats and Countermeasures](#) , ACM SIGCOMM Computer Communication Review 2013
- T. Lauinger, N. Laoutaris, P. Rodriguez, T. Strufe, E. Biersack, E. Kirda, [Privacy risks in named data networking: what is the cost of performance?](#) , ACM SIGCOMM Computer Communication Review 2012.

- S. Arianfar, T. Koponen, B. Raghavan, S. Shenker, [On Preserving Privacy in Content-Oriented Networks](#) , ACM SIGCOMM ICN 2011.

Topic 29: Cloud Security

- S. Bugiel, S. Nurnberger, T. Poppelmann, A. Sadeghi, T. Schneider, [AmazonIA: when elasticity snaps back](#), ACM CCS 2011. **Primary:**
- T. Lauinger, N. Laoutaris, P. Rodriguez, T. Strufe, E. Biersack, E. Kirda, [Resource-Freeing Attacks: Improve Your Cloud Performance \(at Your Neighbor's Expense\)](#) ACM CCS 2012. **Secondary:**
- Z. Wu, Z. Xu, H. Wang, [Whispers in the hyper-space: high-speed covert channel attacks in the cloud](#), USENIX Security 2012.
- M. Almorsy, J. Grundy, A.S. Ibrahim, [Collaboration-Based Cloud Computing Security Management Framework](#), IEEE CLOUD 2011.

Topic 30: Anonymity in Wireless Network

- C.A. Ardagna, M. Conti, M. Leone, J. STEFA, [An Anonymous End-to-End Communication Protocol for Mobile Cloud Environments](#), IEEE Transactions on Services Computing, 2014 **Primary:**
- R. Song, L. Korba, G.Yee, [Anondsr:efficient anonymous dynamic source routing for mobile ad-hoc networks](#), ACM SASN, 2005. **Secondary:**
- X. Lu, P. Hui, D. Towsley, J. Pu, Z. Xiong, [Anti-localization anonymous routing for delay tolerant network](#), Computer Networks 2010.

Topic 31: Smartphone User Profiling

- K. Xu, Z. Zhang, S. Bhattacharyya, [Internet Traffic Behavior Profiling for Network Security Monitoring](#) , IEEE/ACM Transactions on Networking, 2008 **Primary:**
- S. Dai, A. Tongaonkar, X. Wang, A. Nucci, and D. Song, [NetworkProfiler: Towards Automatic Fingerprinting of Android Apps](#) , IEEE INFOCOM 2013. **Secondary:**
- F. Zhang, W. He, X. Liu, P.G. Bridges, [Inferring users' online activities through traffic analysis](#) , ACM WiSec 2011.
- T. Karagiannis, K. Papagiannaki, [BLINC: multilevel traffic classification in the dark](#) , ACM SIGCOMM Computer 2005.
- T. Stober, M. Frank, I. Martinovic and J. Schmitt, [Who do you sync you are? Smartphone Fingerprinting based on Application Behaviour](#) , ACM WiSec 2013.

Topic 32: SSL security issues in Android

- S. Fahl, M. Harbacj, T. Muders, M. Smith, [Why Eve and Mallory Love Android: An Analysis of Android SSL \(In\)Security](#) , Proceedings of the 2012 ACM conference on Computer and communications security (ACM CCS 2012). **Primary:**
- **Secondary:**

- M. Georgiev, S. Iyengar, S. Jana, R. Anubhai, D. Boneh, V Shmatikov, [The most dangerous code in the world: validating SSL certificates in non-browser software](#) , Proceedings of the 2012 ACM conference on Computer and communications security (ACM CCS 2012),
- M. Conti, N. Dragoni, S. Gottardo, [MITHYS: Mind The Hand You Shake](#) , Security and Trust Management. Springer 2013,

Topic 33: Circumvent censorship

Primary:

- K. Xu, Z. Zhang, S. Bhattacharyya, [Protocol Misidentification Made Easy with Format-Transforming Encryption](#), Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security (ACM CCS 2013).

Secondary:

- A. Houmansadr, G. T. K. Nguyen, M. Caesar, N. Borisov, [Cirripede: Circumvention Infrastructure using Router Redirection with Plausible Deniability](#), Proceedings of the 18th ACM conference on Computer and communications security (ACM CCS 2011).
- A. Houmansadr, T. Ridel, N. Borisov, A. Singer, [I want my voice to be heard: IP over Voice-over-IP for unobservable censorship circumvention](#), The 20th Annual Network and Distributed System Security Symposium (NDSS 2013).