Journal of Computer Security 21 (2013) 1009–1012
IOS Press

Author Index Volume 21 (2013)

The issue number is given in front of the page numbers.

Acar, U.A., A. Ahmed, J. Cheney and R. Perera, A core calculus for provenance (6) 919– 969

Ahmed, A., see Acar, U.A. (6) 919– 969

Arapinis, M., S. Bursuc and M. Ryan, Privacy-supporting cloud computing by in-browser key translation (6) 847– 880

Baron, J., K. El Defrawy, K. Minkovich, R. Ostrovsky and E. Tressler, 5PM: Secure pattern matching (5) 601– 625

Barthe, G., B. Grégoire, S. Heraud, F. Olmedo and S. Zanella-Béguelin, Verified indifferentiable hashing into elliptic curves (6) 881– 917

Basin, D., C. Cremers and S. Meier, Provably repairing the ISO/IEC 9798 standard for entity authentication (6) 817– 846

Basin, D., see Meier, S. (1) 41– 87

Bilogrevic, I., see Jadliwala, M. (3) 317– 346

Blanchet, B., see Paiola, M. (6) 781– 816

Blazy, O., G. Fuchsbauer, D. Pointcheval and D. Vergnaud, Short blind signatures (5) 627– 661

Bursuc, S., see Arapinis, M. (6) 847– 880

Centenaro, M., R. Focardi and F.L. Luccio, Type-based analysis of key management in PKCS#11 cryptographic devices (6) 971–1007

Cheney, J., see Acar, U.A. (6) 919– 969

Cortier, V. and B. Smyth, Attacking and fixing Helios: An analysis of ballot secrecy (1) 89– 148

Cremers, C., see Basin, D. (6) 817– 846

Cremers, C., see Meier, S. (1) 41– 87

Cuppens, F., N. Cuppens-Boulahia and Y. Elrakaiby, Formal specification and management of security policies with collective group obligations (1) 149– 190

Cuppens-Boulahia, N., see Cuppens, F. (1) 149– 190

Dawalbhakta, A., see Phatak, D. (2) 233– 281

De Capitani di Vimercati, S., S. Foresti, S. Paraboschi, G. Pelosi and P. Samarati, Supporting concurrency and multiple indexes in private access to outsourced data (3) 425– 461

Degano, P. and J.D. Guttman, Preface (6) 779– 780

Desnoyers, P., see Zhou, F. (4) 533– 559

Down, D.G., see Yarmand, M.H. (1) 1– 39

Du, Y., see Homer, J. (4) 561– 597

El Defrawy, K., see Baron, J. (5) 601– 625

Elrakaiby, Y., see Cuppens, F. (1) 149– 190

0926-227X/13/$27.50 © 2013 – IOS Press and the authors. All rights reserved

Focardi, R., see Centenaro, M. (6) 971–1007
Foresti, S., see De Capitani di Vimercati, S. (3) 425– 461
Fuchsbauer, G., see Blazy, O. (5) 627– 661

Geigel, A., Neural network Trojan (2) 191– 232
Gentry, C., S. Halevi, C. Peikert and N.P. Smart, Field switching in BGV-style homomorphic encryption (5) 663– 684
Goel, M., see Zhou, F. (4) 533– 559
Grégoire, B., see Barthe, G. (6) 881– 917
Guttman, J.D., see Degano, P. (6) 779– 780

Halevi, S., see Gentry, C. (5) 663– 684
Heraud, S., see Barthe, G. (6) 881– 917
Herzberg, A. and R. Margulies, Forcing Johnny to login safely (3) 393– 424
Hicks, M., see Mardziel, P. (4) 463– 532
Homer, J., S. Zhang, X. Ou, D. Schmidt, Y. Du, S.R. Rajagopalan and A. Singhal, Aggregating vulnerability metrics in enterprise networks using attack graphs (4) 561– 597
Hubaux, J.-P., see Jadliwala, M. (3) 317– 346

Jadliwala, M., I. Bilogrevic and J.-P. Hubaux, Optimizing mix-zone coverage in pervasive wireless networks (3) 317– 346
Joshi, N., see Phatak, D. (2) 233– 281

Kobsa, A., R. Nithyanand, G. Tsudik and E. Uzun, Can Jannie verify? Usability of display-equipped RFID tags for security purposes (3) 347– 370
Kolesnikov, V., A.-R. Sadeghi and T. Schneider, A systematic approach to practically efficient general two-party secure function evaluation protocols and their modular design (2) 283– 315
Kreitz, G., Flow stealing: A well-timed redirection attack (3) 371– 391

Lipmaa, H. and B. Zhang, A more efficient computationally sound non-interactive zero-knowledge shuffle argument (5) 685– 719
Luccio, F.L., see Centenaro, M. (6) 971–1007

Magill, S., see Mardziel, P. (4) 463– 532
Manulis, M., see Nieto, J.G. (5) 749– 778
Mardziel, P., S. Magill, M. Hicks and M. Srivatsa, Dynamic enforcement of knowledge-based security policies using probabilistic abstract interpretation (4) 463– 532
Margulies, R., see Herzberg, A. (3) 393– 424
Meier, S., C. Cremers and D. Basin, Efficient construction of machine-checked symbolic protocol security proofs (1) 41– 87
Meier, S., see Basin, D. (6) 817– 846
Minkovich, K., see Baron, J. (5) 601– 625
Myers, S., M. Sergi and a. shelat, Black-box construction of a more than non-malleable CCA1 encryption scheme from plaintext awareness (5) 721– 748

Nieto, J.G., M. Manulis, B. Poettering, J. Rangasamy and D. Stebila, Publicly verifiable ciphertexts (5) 749– 778
Nithyanand, R., see Kobsa, A. (3) 347– 370

Olmedo, F., see Barthe, G. (6) 881– 917
Ostrovsky, R., see Baron, J. (5) 601– 625
Ou, X., see Homer, J. (4) 561– 597

Paiola, M. and B. Blanchet, Verification of security protocols with lists: From length one to unbounded length (6) 781– 816
Paraboschi, S., see De Capitani di Vimercati, S. (3) 425– 461
Peikert, C., see Gentry, C. (5) 663– 684
Pelosi, G., see De Capitani di Vimercati, S. (3) 425– 461
Perera, R., see Acar, U.A. (6) 919– 969
Phatak, D., A.T. Sherman, N. Joshi, B. Sonawane, V.G. Relan and A. Dawalbhakta, Spread Identity: A new dynamic address remapping mechanism for anonymity and DDoS defense (2) 233– 281
Poettering, B., see Nieto, J.G. (5) 749– 778
Pointcheval, D., see Blazy, O. (5) 627– 661

Rajagopalan, S.R., see Homer, J. (4) 561– 597
Rangasamy, J., see Nieto, J.G. (5) 749– 778
Relan, V.G., see Phatak, D. (2) 233– 281
Ryan, M., see Arapinis, M. (6) 847– 880

Sadeghi, A.-R., see Kolesnikov, V. (2) 283– 315
Samarati, P., see De Capitani di Vimercati, S. (3) 425– 461
Sartipi, K., see Yarmand, M.H. (1) 1– 39
Schmidt, D., see Homer, J. (4) 561– 597
Schneider, T., see Kolesnikov, V. (2) 283– 315
Sergi, M., see Myers, S. (5) 721– 748
shelat, a., see Myers, S. (5) 721– 748
Sherman, A.T., see Phatak, D. (2) 233– 281
Singhal, A., see Homer, J. (4) 561– 597
Smart, N.P., see Gentry, C. (5) 663– 684
Smyth, B., see Cortier, V. (1) 89– 148
Sonawane, B., see Phatak, D. (2) 233– 281
Srivatsa, M., see Mardziel, P. (4) 463– 532
Stebila, D., see Nieto, J.G. (5) 749– 778
Sundaram, R., see Zhou, F. (4) 533– 559

Tressler, E., see Baron, J. (5) 601– 625
Tsudik, G., see Kobsa, A. (3) 347– 370

Uzun, E., see Kobsa, A. (3) 347– 370

Vergnaud, D., see Blazy, O. (5) 627– 661
Visconti, I., Guest Editor's preface (5) 599– 600

Yarmand, M.H., K. Sartipi and D.G. Down, Behavior-based access control for distributed healthcare systems (1) 1– 39

Zanella-Béguelin, S., see Barthe, G. (6) 881– 917

Zhang, B., see Lipmaa, H. (5) 685– 719

Zhang, S., see Homer, J. (4) 561– 597

Zhou, F., M. Goel, P. Desnoyers and R. Sundaram, Scheduler vulnerabilities and coordinated attacks in cloud computing (4) 533– 559