Publications

Prof. **N. Asokan**

November 2018

A Peer-reviewed scientific articles

A1 Journal article (refereed), original research

1. Ágnes Kiss, Masoud Naderpour, Jian Liu, **N. Asokan**, Thomas Schneider: SoK: Modular and Efficient Private Decision Tree Evaluation, Proceedings on Privacy Enhancing Technologies (PoPETs), (to appear) 2019
2. Markus Miettinen, **N.** Asokan: Ad-hoc key agreement: A brief history and the challenges ahead, Computer Communications, 2018. https://doi.org/10.1016/j.comcom.2018.07.030
3. Elena Reshetova, Hans Liljestrand, Andrew Paverd, **N.** Asokan: Towards Linux Kernel Memory Safety, Software Practice and Experience, 2018. https://doi.org/10.1002/spe.2638
4. N**. Asokan**, Thomas Nyman, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, Gene Tsudik: ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices, (to appear in) IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems (TCAD), 37(11): 2290-2300 (2018). https://doi.org/10.1109/TCAD.2018.2858422
5. Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, **N. Asokan**: Sensor-based Proximity Detection in the Face of Active Adversaries, IEEE Transactions on Mobile Computing, 2018 https://doi.org/10.1109/TMC.2018.2839604
6. Jian Liu, Wenting Li, Ghassan Karame, **N. Asokan**: Toward fairness of cryptocurrency payments, IEEE Security & Privacy, May/June (2018) http://doi.ieeecomputersociety.org/10.1109/MSP.2018.2701163
7. Andrew Paverd, Sandeep Tamrakar, Hoang Long Nguyen, Praveen Pendyala, Thien Duc Nguyen, Elizabeth Stobert, Tommi Gröndahl, **N. Asokan**, Ahmad-Reza Sadeghi: OmniShare: Encrypted Cloud Storage for the Multi-Device Era, IEEE Internet Computing (2018). http://dx.doi.org/10.1109/MIC.2018.182130646
8. Ágnes Kiss, Jian Liu, Thomas Schneider, **N. Asokan**, Benny Pinkas: Private Set Intersection for Unequal Set Sizes with Mobile Applications, Proceedings on Privacy Enhancing Technologies (PoPETs), 2017(4):97-117, https://doi.org/10.1515/popets-2017-0044
9. Samuel Marchal, Giovanni Armano, Tommi Gröndahl, Kalle Saari, Nidhi Singh, **N. Asokan**: Off-the-Hook: An Efficient and Usable Client-Side Phishing Prevention Application. IEEE Transactions on Computers, https://doi.org/10.1109/TC.2017.2703808
10. Tooska Dargahi, Moreno Ambrosin, Mauro Conti, **N. Asokan**: ABAKA: A novel attribute-based k-anonymous collaborative solution for LBSs. Computer Communications 85: 1-13 (2016). http://dx.doi.org/10.1016/j.comcom.2016.03.002
11. Hien Thi Thu Truong, Xiang Gao, Babins Shrestha, Nitesh Saxena, **N. Asokan**, Petteri Nurmi: Using contextual co-presence to strengthen Zero-Interaction Authentication: Design, integration and usability. Pervasive and Mobile Computing, Volume 16, Part B, January 2015, Pages 187–204. http://dx.doi.org/10.1016/j.pmcj.2014.10.005

12. **N Asokan**, Jan-Erik Ekberg, Kari Kostiainen, Anand Rajan, Carlos V. Rozas, Ahmad-Reza Sadeghi, Steffen Schulz, Christian Wachsmann: Mobile Trusted Computing. Proceedings of the IEEE 102(8): 1189-1206 (2014). http://dx.doi.org/10.1109/JPROC.2014.2332007
13. Jan-Erik Ekberg, Kari Kostiainen, **N. Asokan**: The Untapped Potential of Trusted Execution Environments on Mobile Devices, IEEE Security & Privacy Magazine, 2014. http://dx.doi.org/10.1109/MSP.2014.38
14. Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, **N. Asokan**: Secure Device Pairing based on a Visual Channel, IEEE Trans. Information Forensics and Security 6(1):28-38. 2011. http://dx.doi.org/10.1109/TIFS.2010.2096217
15. John Solis, **N. Asokan**, Kari Kostiainen, Philip Ginzboorg, Jörg Ott: Controlling Resource Hogs in Delay-Tolerant Networks, Computer Communications, 33:1, 2-10, 2010. http://dx.doi.org/10.1016/j.comcom.2009.07.019
16. Jani Suomalainen, Jukka Valkonen, **N. Asokan**: Standards for Security Associations in Personal Networks: A Comparative Analysis, International Journal of Security and Networks (IJSN), special issue on Secure Spontaneous Interaction, 2009. http://dx.doi.org/10.1504/IJSN.2009.023428
17. Philip Ginzboorg, **N. Asokan**: Key Agreement in Ad-hoc Networks, Computer Communications, Special issue on security, 23 (2000):1627-1637, 2000. http://dx.doi.org/10.1016/S0140-3664(00)00249-8
18. **N. Asokan,** Hervé Debar, Michael Steiner, Michael Waidner: Authenticating Public Terminals, Computer Networks, 31(8):861-870, May 1999. http://dx.doi.org/10.1016/S1389-1286(98)00020-6
19. Günter Karjoth, **N. Asokan,** Ceki Gülcü: Protecting the Computation Results of Free-roaming Agents, Personal Ubiquitous Computing, 2(2):92-99, December 1998. http://dx.doi.org/10.1007/BF01324939
20. **N. Asokan**, Victor Shoup, Michael Waidner: Optimistic Fair Exchange of Digital Signatures, IEEE Journal on Selected Areas in Communications, 18(4):593-610, April 2000. http://dx.doi.org/10.1109/49.839935
21. J. L. Abad-Peiro, **N. Asokan**, , Michael Steiner, Michael Waidner: Designing a Generic Payment Service, IBM Systems Journal, 37(1):72-88, January 1998. http://dx.doi.org/10.1147/sj.371.0072
22. **N. Asokan**, Gene Tsudik, Michael Waidner: Server-supported Signatures. Journal of Computer Security, 5(1):91-108, 1997. http://dx.doi.org/10.3233/JCS-1997-5105

A2 Review article, Literature review, Systematic review

23. **N. Asokan**, Phil Janson, Michael Steiner, Michael Waidner: State of the Art in Electronic Payment Systems, IEEE Computer, 30(9):28-35, September 1997. http://doi.ieeecomputersociety.org/10.1109/2.612244: **Translation: (in Japanese)** Nikkei Computer, pages 195-201, issue of March 30, 1998.

A3 Book section, chapters in research books

24. **N. Asokan**, Kaisa Nyberg: Security Associations for Personal Devices, (**Invited** book chapter) in S. Gritzalis et al. (Editors), "Security and Privacy in Wireless and Mobile Networking", (preprint at http://research.ics.tkk.fi/publications/knyberg/secass.pdf), Troubador Publishing, 2008, ISBN 978-1905886-906, http://www.troubador.co.uk/book_info.asp?bookid=428
25. **N. Asokan**, Matthias Schunter: Optimistic Fair Exchange (**Invited** book chapter) in H. Raghav Rao and Shambhu Upadhyay (editors), Information Assurance, Security and Privacy Services,

Emerald Group Publishing Ltd., May 2009, pages 365-390. https://books.google.com/books?isbn=1848551940

26. **N. Asokan**, Jan-Erik Ekberg: Mobile Digital Rights Management (book chapter) in Professional MITA – Visions and Implementations, edited by Nokia, IT Press, 2002.
27. **N. Asokan**, Phil Janson, Michael Steiner, Michael Waidner: State of the Art in Electronic Payment Systems, (**Invited** book chapter) in Advances in Computers, Vol. 53, pages 425-449, Edited by Marvin. V. Zelkowitz, Academic Press, March 2000. http://dx.doi.org/10.1016/S0065-2458(00)80009-1

A4 Conference proceedings

28. Tommi Gröndahl, Luca Pajola, Mika Juuti, Mauro Conti, **N. Asokan**: All you need is "love": Evading hate speech detection, AISec, 2018. https://doi.org/10.1145/3270101.3270103
29. Mika Juuti, Bo Sun, Tatsuya Mori and **N. Asokan**: Stay On-Topic: Generating Context-specific Fake Restaurant Reviews, European Symposium on Research in Computer Security (ESORICS), 2018. https://doi.org/10.1007/978-3-319-99073-6_7
30. Samuel Marchal, **N. Asokan**: On Designing and Evaluating Phishing Webpage Detection Techniques for the Real World. CSET @ USENIX Security Symposium 2018, https://www.usenix.org/conference/cset18/presentation/marchal
31. A Kurnikov, A Paverd, M Mannan, **N Asokan**: Keys in the Clouds: Auditable Multi-device Access to Cryptographic Credentials, Workshop on Security, Privacy, Identity Management in the Cloud (SECPID). 2018. http://doi.acm.org/10.1145/3230833.3234518
32. Fritz Alder, Arseny Kurnikov, Andrew Paverd, **N. Asokan**: Migrating SGX Enclaves with Persistent State. Distributed Systems and Networks (DSN) 2018. https://doi.org/10.1109/DSN.2018.00031
33. Markus Miettinen, Thien Duc Nguyen, Ahmad-Reza Sadeghi, **N. Asokan**: Revisiting context-based authentication in IoT. DAC 2018: 32:1-32:6 http://doi.acm.org/10.1145/3195970.3196106
34. Chris Vaas, Mika Juuti, **N. Asokan**, Ivan Martinovic: Get in Line: Ongoing Co-Presence Verification of a Vehicle Formation Based on Driving Trajectories, IEEE Euro S&P, 2018. https://doi.org/10.1109/EuroSP.2018.00022
35. Jian Liu, Duan Li, Yong Li, **N. Asokan**: Secure Deduplication of Encrypted Data: Refined Model and New Constructions, CT-RSA 2018:374-393. https://doi.org/10.1007/978-3-319-76953-0_20
36. Arseny Kurnikov, Klaudia Krawiecka, Andrew Paverd, Mohammad Mannan, **N. Asokan**: Using SafeKeeper to Protect Web Passwords. WWW (Companion Volume) 2018: 159-162, http://doi.acm.org/10.1145/3184558.3186968
37. Klaudia Krawiecka, Arseny Kurnikov, Andrew Paverd, Mohammad Mannan, **N. Asokan**: SafeKeeper: Protecting Web Passwords using Trusted Execution Environments. World Wide Web conference 2018. https://doi.org/10.1145/3178876.3186101
38. Jian Liu, Mika Juuti, Yao Lu, **N. Asokan**: Oblivious Neural Network Predictions via MiniONN Transformations. CCS 2017: 619-631, http://doi.acm.org/10.1145/3133956.3134056
39. Elena Reshetova, Filippo Bonazzi, **N. Asokan**: Randomization Can't Stop BPF JIT Spray. NSS 2017: 233-247, https://doi.org/10.1007/978-3-319-64701-2_17
40. Thomas Nyman, Jan-Erik Ekberg, Lucas Davi, **N. Asokan:** CFI CaRE: Hardware-supported Call and Return Enforcement for Commercial Microcontrollers, in RAID 2017: 259-2847. https://doi.org/10.1007/978-3-319-66332-6_12

41. Ghada Dessouky, Shaza Zeitouni, Thomas Nyman, Andrew Paverd, Lucas Davi, Patrick Koeberl, **N. Asokan**, Ahmad-Reza Sadeghi: LO-FAT: Low-Overhead Control Flow ATtestation in Hardware. DAC 2017: 24:1-24:6, http://doi.acm.org/10.1145/3061639.3062276
42. Radek Tomsu, Samuel Marchal, **N. Asokan**: Profiling Users by Modeling Web Transactions. IEEE ICDCS 2017: 2399-2404, Atlanta, GA, June 2017, https://doi.org/10.1109/ICDCS.2017.164
43. Markus Miettinen, Samuel Marchal, Ibbad Hafeez, Tommaso Frassetto, **N. Asokan**, Ahmad-Reza Sadeghi, Sasu Tarkoma: IoT Sentinel Demo: Automated Device-Type Identification for Security Enforcement in IoT. IEEE ICDCS 2017: 2511-2514, Atlanta, GA, June 2017, https://doi.org/10.1109/ICDCS.2017.284 **(Best demo/poster)**
44. Markus Miettinen, Samuel Marchal, Ibbad Hafeez, **N. Asokan**, Ahmad-Reza Sadeghi, Sasu Tarkoma: IoT SENTINEL: Automated Device-Type Identification for Security Enforcement in IoT. IEEE ICDCS 2017: 2177-2184, Atlanta, GA, June 2017, https://doi.org/10.1109/ICDCS.2017.283
45. Mika Juuti, Christian Vaas, Ivo Sluganovic, Hans Liljestrand, **N. Asokan**, Ivan Martinovic: STASH: Securing transparent authentication schemes using prover-side proximity verification. IEEE International Conference on Sensing, Communication and Networking (SECON), San Diego, CA, June 2017, https://doi.org/10.1109/SAHCN.2017.7964922
46. Sandeep Tamrakar, Jian Liu, Andrew Paverd, Jan-Erik Ekberg, Benny Pinkas, **N. Asokan**: The Circle Game: Scalable Private Membership Test Using Trusted Hardware. ACM Asia Conference on Computer and Communications Security (ACM ASIACCS), Abu Dhabi, UAE, April 2017 (**Honorable Mention**), https://doi.org/10.1145/3052973.3053006
47. Elena Reshetova, Filippo Bonazzi, **N. Asokan**: SELint: an SEAndroid policy analysis tool. ICISSP 2017: 47-58, https://doi.org/10.5220/0006126600470058
48. Klaudia Krawiecka, Andrew Paverd, **N. Asokan**: Protecting Password Databases using Trusted Hardware. SysTEX@Middleware 2016: 9:1-9:6, http://doi.acm.org/10.1145/3007788.3007798
49. Kubilay Ahmet Küçük, Andrew Paverd, Andrew C. Martin, **N. Asokan**, Andrew Simpson, Robin Ankele: Exploring the use of Intel SGX for Secure Many-Party Applications. SysTEX@Middleware 2016: 5:1-5:6, http://doi.acm.org/10.1145/3007788.3007793
50. Tigist Abera, N. Asokan, Lucas Davi, Jan-Erik Ekberg, Thomas Nyman, Andrew Paverd, Ahmad-Reza Sadeghi, Gene Tsudik: C-FLAT: Control-FLow ATtestation for Embedded Systems Software. ACM Conference on Computer and Communicatiosn Security (ACM CCS), Vienna, Austria, 2016, http://doi.acm.org/10.1145/2976749.2978358
51. Tigist Abera, N. Asokan, Lucas Davi, Farinaz Koushanfar, Andrew Paverd, Ahmad-Reza Sadeghi, Gene Tsudik: Invited - Things, trouble, trust: on building trust in IoT systems. DAC 2016: 121:1-121:6, http://doi.acm.org/10.1145/2897937.2905020
52. Elena Reshetova, Filippo Bonazzi, Thomas Nyman, Ravishankar Borgaonkar, **N. Asokan**: Characterizing SEAndroid Policies in the Wild. ICISSP 2016: 482-489, http://dx.doi.org/10.5220/0005759204820489
53. Narges Yousefnezhad, Marcin Nagy, **N. Asokan**: On improving tie strength estimates by aggregating multiple communication channels. Networking 2016: 530-535, http://dx.doi.org/10.1109/IFIPNetworking.2016.7497255
54. Samuel Marchal, Kalle Saari, Nidhi Gupta, **N. Asokan**: Know Your Phish: Novel Techniques for Detecting Phishing Sites and their Targets, 36th IEEE International Conference on Distributed Computing Systems (ICDCS), June 2016, http://dx.doi.org/10.1109/ICDCS.2016.10
55. Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena, **N. Asokan**: Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks, Networks and Distributed Systems Conference (NDSS), February 2016, http://www.internetsociety.org/sites/default/files/blogs-media/pitfalls-designing-zero-effort-deauthentication-opportunistic-human-observation-attacks.pdf

56. Altaf Shaik, Ravishankar Borgaonkar, **N. Asokan**, Valtteri Niemi, Jean-Pierre Seifert: Practical attacks against privacy and availability in 4G/LTE mobile communication systems, Networks and Distributed Systems Conference (NDSS), February 2016. http://www.internetsociety.org/sites/default/files/blogs-media/practical-attacks-against-privacy-availability-4g-lte-mobile-communication-systems.pdf
57. Jian Liu, **N. Asokan,** Benny Pinkas: Secure Deduplication of Encrypted Data without Additional Independent Servers. 2015 ACM Conference on Computer and Communications Security (ACM CCS), Denver, Colorado, October 2015. http://doi.acm.org/10.1145/2810103.2813623
58. Jian Liu, **N. Asokan,** Benny Pinkas: Secure Deduplication of Encrypted Data without Additional Independent Servers. 2015 ACM Conference on Computer and Communications Security (ACM CCS), Denver, Colorado, October 2015. http://doi.acm.org/10.1145/2810103.2813623
59. **N. Asokan**, Ferdinand Brasser, Ahmad Ibrahim, Ahmad-Reza Sadeghi, Matthias Schunter, Gene Tsudik, Christian Wachsmann, SEDA: Scalable Embedded Device Attestation. 2015 ACM Conference on Computer and Communications Security (ACM CCS), Denver, Colorado, October 2015. http://doi.acm.org/10.1145/2810103.2813670
60. Imtiaj Ahmad, Yina Ye, Sourav Bhattacharya, **N. Asokan,** Giulio Jacucci, Petteri Nurmi, Sasu Tarkoma: Checksum Gestures: Continuous Gestures as an Out-of-Band Channel for Secure Pairing. 2015 ACM International Joint Conference on Pervasive and Ubiquitous Computing (ACM UbiComp 2015), Osaka, Japan, September 2015. http://doi.acm.org/10.1145/2750858.2807521
61. Thomas Nyman, Brian McGillion, **N. Asokan**: On Making Emerging Trusted Execution Environments Accessible to Developers, 8th International Conference of Trust & Trustworthy Computing (TRUST 2015), Heraklion, Crete, Greece, August 24-26, 2015, http://dx.doi.org/10.1007/978-3-319-22846-4_4
62. Brian McGillion, Tanel Dettenborn, Thomas Nyman, **N. Asokan**: Open-TEE - An Open Virtual Trusted Execution Environment, 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE TrustCom 2015), Helsinki, Finland, August 20-22, 2015, http://dx.doi.org/10.1109/Trustcom.2015.400
63. Marcin Nagy, Thanh Bui, Emiliano De Cristofaro, **N. Asokan**, Joerg Ott, Ahmad-Reza Sadeghi: How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length with Social PaL. 8th ACM Conference on Security and Privacy in Wireless and Mobile Networks (ACM WiSec), New York, June 2015. http://doi.acm.org/10.1145/2766498.2766501
64. Markus Miettinen, **N. Asokan**, Farinaz Koushanfar, Thien Duc Nguyen, Jon Rios, Ahmad-Reza Sadeghi, Majid Sobhani, Sudha Yellapantula: I Know Where You are: Proofs of Presence Resilient to Malicious Provers. 10th ACM Symposium on Information, Computer and Communications Security (ACM ASIACCS), Singapore, April 2015. http://doi.acm.org/10.1145/2714576.2714634
65. Christoph Busold, Stephan Heuser, Jon Rios, Ahmad-Reza Sadeghi, N. Asokan: Smart and Secure Cross-Device Apps for the Internet of Advanced Things. Financial Cryptography 2015: 272-290, http://dx.doi.org/10.1007/978-3-662-47854-7_17
66. Thomas Nyman, Jan-Erik Ekberg, **N. Asokan**: Citizen Electronic Identities using TPM 2.0. ACM TrustED@CCS 2014: 37-48 http://doi.acm.org/10.1145/2666141.2666146
67. Markus Miettinen, **N. Asokan**, Thien Duc Nguyen, Ahmad-Reza Sadeghi and Majid Sobhani: Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Device, 21st ACM Conference on Computer and Communications Security (ACM CCS), Scottsdale, Arizona, November 2014. http://doi.acm.org/10.1145/2660267.2660334
68. Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, **N. Asokan**: ConXsense – Context Profiling and Classification for Context-Aware Access Control, 9th ACM Symposium on

Information, Computer and Communications Security (ACM ASIACCS), Kyoto, Japan, June 2014 (**Best paper award**). http://doi.acm.org/10.1145/2590296.2590337

69. Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, N. Asokan: Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-sensing. Financial Cryptography 2014: 349-364. http://dx.doi.org/10.1007/978-3-662-45472-5_23
70. Eemil Lagerspetz, Hien Thi Thu Truong, Sasu Tarkoma, **N. Asokan**: MDoctor: A Mobile Malware Prognosis Application. ICDCS Workshops 2014: 201-206. http://dx.doi.org/10.1109/ICDCSW.2014.36
71. Jian Liu, Sini Ruohomaa, Kumaripaba Athukorala, Giulio Jacucci, **N. Asokan**, Janne Lindqvist: Groupsourcing: nudging users away from unsafe content. NordiCHI 2014: 883-886. http://doi.acm.org/10.1145/2639189.2670184
72. Elena Reshetova, Janne Karhunen, Thomas Nyman, **N. Asokan**: Security of OS-Level Virtualization Technologies. NordSec 2014: 77-93. http://dx.doi.org/10.1007/978-3-319-11599-3_5
73. Hien Thi Thu Truong, Eemil Lagerspetz, Petteri Nurmi, Adam J. Oliner, Sasu Tarkoma, **N. Asokan**, Sourav Bhattacharya: The Company You Keep: Mobile Malware Infection Rates and Inexpensive Risk Indicators, Proceedings of the 23rd International World Wide Web Conference (WWW 2014), Seoul, Korea, April 2014. http://dx.doi.org/10.1145/2566486.2568046
74. Hien Truong, Xiang Gao, Babins Shrestha, Nitesh Saxena, **N. Asokan**, Petteri Nurmi: Comparing and Fusing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication, Proceedings of the IEEE International Conference on Pervasive Computing and Communications (IEEE PerCom), Budapest, Hungary, March 2014. http://dx.doi.org/10.1109/PerCom.2014.6813957
75. Babins Shrestha, Nitesh Saxena, Hien Truong, **N. Asokan**: Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing, Financial Cryptography and Data Security (FC 2014), Barbados, March 2014. http://dx.doi.org/10.1007/978-3-662-45472-5_23
76. Marcin Nagy, Alexandra Dimitrienki, Emiliano De Cristofaro, Ahmad-Reza Sadeghi, **N. Asokan**: Do I know you?: Efficient and Privacy-Preserving Common Friend-Finder Protocols and Applications, Proceedings of the Annual Computer Security Applications Conference (ACSAC), New Orleans, December 2013. http://dx.doi.org/10.1145/2523649.2523668
77. Marcin Nagy, **N. Asokan**, Jörg Ott: PeerShare: A System Secure Distribution of Sensitive Data Among Social Contacts, Proceedings of Nordsec 2013, Ilulissat, Greenland, October 2013, Lecture Notes in Computer Science 8208, pp 154-165. http://dx.doi.org/10.1007/978-3-642-41488-6_11
78. **N. Asokan**, Alexandra Dmitrienko, Marcin Nagy, Elena Reshetova, Ahmad-Reza Sadeghi, Thomas Schneider, Stanislaus Stelle: CrowdShare: Secure Mobile Resource Sharing , Proceedings of ACNS 2013, Banff, AB, Canada, June 2013, Lecture Notes in Computer Science 7954, pp 432-440. http://dx.doi.org/10.1007/978-3-642-38980-1_27
79. Aditi Gupta, Markus Miettinen, Marcin Nagy, **N. Asokan**: Intuitive security policy configuration in mobile devices using context profiling, Proceedings of the SocialCom 2012 Conference, Amsterdam, The Netherlands, September 2012. http://dx.doi.org/10.1109/SocialCom-PASSAT.2012.60
80. Jan-Erik Ekberg, Alexandra Afanasyeva , **N. Asokan**: Authenticated encryption primitives for size-constrained trusted computing, Proceedings of the Fifth International Conference on Trust and Trustworthy Computing (TRUST), Vienna, Austria, June 2012. http://dx.doi.org/10.1007/978-3-642-30921-2_1

81. Pern Hui Chia, Yusuke Yamamoto, **N. Asokan**: Is this app safe?: a large scale study on application permissions and risk, Proceedings of the 21st international conference on World Wide Web (WWW 2012), Lyon, France, April 2012. http://dx.doi.org/10.1145/2187836.2187879
82. Aditi Gupta, Markus Miettinen, Marcin Nagy, **N. Asokan**, Alexandre Wetzel: PeerSense: who is near you? IEEE PerCom Workshops 2012: 516-518. http://dx.doi.org/10.1109/PerComW.2012
83. Aditi Gupta, Markus Miettinen, **N. Asokan**: Using context-profiling to aid access control decisions in mobile devices. IEEE PerCom Workshops 2011: 310-312 **(Best demo award)**, http://dx.doi.org/10.1109/PERCOMW.2011
84. John Solis, Philip Ginzboorg, **N. Asokan**, Jörg Ott: Best effort authentication for opportunistic networks, HotWisec 2011, Proceedings of the 30th IEEE International Performance Computing and Communications Conference, Orlando, Florida, November 2011. http://doi.ieeecomputersociety.org/10.1109/PCCC.2011.6108110
85. Sandeep Tamrakar, Jan-Erik Ekberg, **N. Asokan**: Identity verification schemes for public transport ticketing with NFC phones, Proceedings of the sixth ACM workshop on Scalable trusted computing (STC 2011), Chicago, October 2011. http://dx.doi.org/10.1145/2046582.2046591
86. Kari Kostiainen, **N. Asokan**: Credential life cycle management in open credential platforms, Proceedings of the sixth ACM workshop on Scalable trusted computing (STC 2011), Chicago, October 2011. http://dx.doi.org/10.1145/2046582.2046595
87. Kari Kostiainen, Jan-Erik Ekberg, **N. Asokan**: Practical Property-Based Attestation on Mobile Devices, Proceedings of the 4th International Conference on Trust and Trustworthy Computing (TRUST 2011), Pittsburgh, June 2011. http://dx.doi.org/10.1007/978-3-642-21599-5_6
88. Kari Kostiainen, Alexandra Afanasyeva, **N. Asokan**: Towards User-Friendly Credential Transfer on Open Credential, Proceedings of the 9th International Conference on Applied Cryptography and Network Security (ACNS '11), Malaga, June 2011. http://dx.doi.org/10.1007/978-3-642-21554-4_23
89. Nitesh Saxena, Md. Borhan Uddin, Jonathan Voris, **N. Asokan**: Vibrate-to-unlock: Mobile phone assisted user authentication to multiple personal RFID tags, IEEE International Conference on Pervasive Computing and Communications (PerCom) 2011, Seattle, March 2011. http://dx.doi.org/10.1109/PERCOM.2011.5767583
90. Sandeep Tamrakar, Jan-Erik Ekberg, Pekka Laitinen, **N. Asokan**, Tuomas Aura: Can Hand-held Computers Still be Better Smart Cards? (with Sandeep Tamrakar et al), Proceedings of the Second International Conference on Trusted Systems (INTRUST), Beijing, December 2010. http://dx.doi.org/10.1007/978-3-642-25283-9_14
91. Pern Hui Chia, Andreas Heiner, **N. Asokan**: Use of Ratings from Personalized Community for Trustworthy Application Installation, Proceedings of Nordsec 2010 Conference, Helsinki, October 2010. http://dx.doi.org/10.1007/978-3-642-27937-9_6
92. Kari Kostiainen, **N. Asokan**, Jan-Erik Ekberg: Credential Disabling from Trusted Execution Environments, Proceedings of Nordsec 2010 Conference, Helsinki, October 2010. http://dx.doi.org/10.1007/978-3-642-27937-9_12
93. Markus Miettinen, **N. Asokan**: Towards Security Policy Decisions based on Context Profiling Proceedings of the Third ACM Workshop on Artificial Intelligence and Security (AISec), Chicago, October 2010. http://doi.acm.org/10.1145/1866423.1866428
94. Paul Dunphy, Andreas Heiner , **N. Asokan**: A Closer Look at Recognition-based Graphical Passwords on Mobile Devices, Proceedings of Symposium On Usable Privacy and Security (SOUPS), Redmond, July 2010. http://doi.acm.org/10.1145/1837110.1837114
95. Kari Kostiainen, Alexandra Dmitrienko, Jan-Erik Ekberg and Ahmad-Reza Sadeghi, **N. Asokan**: Key Attestation from Trusted Execution Environments, Proceedings of International Conference on

Trust and Trustworthy Computing (TRUST), Berlin, June 2010. http://dx.doi.org/10.1007/978-3-642-13869-0_3

96. Jan-Erik Ekberg, **N. Asokan**: External Authenticated Non-Volatile Memory with Lifecycle Management for State Protection in Trusted Computing (**Best paper award**), Proceedings of the First International Conference on Trusted Systems (INTRUST), Beijing, December 2009. http://dx.doi.org/10.1007/978-3-642-14597-1_2
97. Kari Kostiainen, Jan-Erik Ekberg, **N. Asokan**, Aarne Rantala: On-board Credentials with Open Provisioning, Proceedings of the ACM ASIACCS conference, March 2009. http://doi.acm.org/10.1145/1533057.1533074
98. Jan-Erik Ekberg, Kari Kostiainen, Aarne Rantala, **N. Asokan**: Scheduling the execution of credentials in constrained secure environments, Proceedings of the Third ACM Workshop on Scalable Trusted Computing (ACM-STC '08), October 2008. http://doi.acm.org/10.1145/1456455.1456465
99. Andreas Heiner, **N. Asokan**: Using Salience Differentials to Making Visual Cues Noticeable, Proceedings of the Usability, Psychology, and Security Workshop (UPSEC '08). http://www.usenix.org/events/upsec08/tech/full_papers/heiner/heiner.pdf
100. Long Nguyen Hoang, Pekka Laitinen, **N. Asokan**: Secure Roaming with Identity Metasystems, Proceedings of the Seventh Symposium on Identity and Trust on the Internet (IDtrust 2008), March 2008. http://doi.acm.org/10.1145/1373290.1373297
101. Jan-Erik Ekberg, **N. Asokan**: A Platform for OnBoard Credentials. (poster paper) Proceedings of the Twelfth International Conference on Financial Cryptography and Data Security (Financial Crypto), January 2008. Volume 5143 of Lecture Notes in Computer Science, Springer. http://dx.doi.org/10.1007/978-3-540-85230-8_31
102. Yacine Gasmi, Ahmad-Reza Sadeghi, Patrick Stewin and Martin Unger, **N. Asokan**: Beyond Secure Channels, Proceedings of the Second ACM Workshop on Scalable Trusted Computing (ACM-STC '07), November 2007. http://doi.acm.org/10.1145/1314354.1314363
103. Ahmad-Reza Sadeghi, Marko Wolf, Christian Stüble, **N. Asokan**, Jan-Erik Ekberg: Enabling Fairer Digital Rights Management with Trusted Computing, Proceedings of the Tenth Information Security Conference (ISC '07), October 2007, Valparaiso, Chile. http://dx.doi.org/10.1007/978-3-540-75496-1_4
104. Andreas Heiner, **N. Asokan**: Secure software installation in a mobile environment, Proceedings of the Third symposium on Usable privacy and security (SOUPS), July 2007. http://doi.acm.org/10.1145/1280680.1280705
105. **N. Asokan**, Kari Kostiainen, Philip Ginzboorg, Jörg Ott, Cheng Luo: Applicability of Identity-based Cryptography for Disruption-Tolerant Networking, Proceedings of the First International MobiSys Workshop on Mobile Opportunistic Networking (MobiOpp), June 2007. http://dx.doi.org/10.1145/1247694.1247705
106. Jani Suomalainen, Jukka Valkonen, **N. Asokan** Security Associations in Personal Networks: A Comparative Analysis, Proceedings of the Fourth European Workshop on Security and Privacy in Ad hoc and Sensor Networks (ESAS), Cambridge, UK, July 2007. Volume 4572 of Lecture Notes in Computer Science, Springer. http://dx.doi.org/10.1007/978-3-540-73275-4_4
107. Ersin Uzun, Kristiina Karvonen, **N. Asokan**: Usability Analysis of Secure Pairing Methods, Proceedings of the Usable Security (USEC) workshop, Scarborough, Trinidad/Tobago, Lecture Notes in Computer Science 4886, Springer 2008. http://dx.doi.org/10.1007/978-3-540-77366-5_29
108. Jukka Valkonen, **N. Asokan**, Kaisa Nyberg: Ad Hoc Security Associations for Groups, Proceedings of the Third European Workshop on Security and Privacy in Ad hoc and Sensor

Networks (ESAS), Hamburg, Germany, September 2006. Volume 4357 of Lecture Notes in Computer Science, Springer. http://dx.doi.org/10.1007/11964254_14

109. Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, **N. Asokan**: Secure Device Pairing based on a Visual Channel, (Short paper) Proceedings of the 2006 IEEE Symposium on Security and Privacy, pages 306--313, Berkeley/Oakland, May 2006. http://doi.ieeecomputersociety.org/10.1109/SP.2006.35
110. Jarkko Tolvanen, Jaakko Lipasti, Tapio Suihko, **N. Asokan**: Remote Storage for Mobile Devices, Proceedings of the First International conference on Communication System Software and Middleware (COMSWARE), New Delhi, India, January 2006. http://dx.doi.org/10.1109/COMSWA.2006.1665195
111. **N. Asokan**, Lauri Tarkkala: Issues in Initializing Security, (**Invited**) Proceedings of the IEEE Symposium on Signal Processing and Information Technology (ISSPIT), Athens, Greece, December 2005. http://dx.doi.org/10.1109/ISSPIT.2005.1577141
112. **N. Asokan**, Seamus Moloney, Philip Ginzboorg, Kari Kostiainen: Visitor Access Management in Personal Wireless Networks, Proceedings of the IEEE International Symposium on Multimedia (ISM2005) Multisec '05Workshop, pages 686-694, 2005. http://doi.ieeecomputersociety.org/10.1109/ISM.2005.122
113. **N. Asokan**, Valtteri Niemi, Pekka Laitinen: On the Usefulness of Proof-of-Possession, Proceedings of the 2nd Annual PKI Research Workshop, Gaithersburg, MD, USA, April 2003. Available at http://middleware.internet2.edu/pki03/presentations/10.pdf
114. **N. Asokan**, Kaisa Nyberg, Valtteri Niemi: Man-in-the-middle in Tunneled Authentication Protocols, Proceedings of the Eleventh International Security Protocols Workshop, volume 3364 of Lecture Notes in Computer Science, pages 28-41, April 2003, Springer. http://dx.doi.org/10.1007/11542322_6
115. Sampo Sovio, **N. Asokan**, Kaisa Nyberg: Defining Authorization Domains Using Virtual Devices, In Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), 2003. http://computer.org/proceedings/saint-w/1873/18730331abs.htm
116. Manel Guerrero Zapata, **N. Asokan**: Securing Ad hoc Routing Protocols, Proceedings of the ACM workshop on Wireless security (WiSE) 2002 , Atlanta, GA, pages 1-10, 2002. http://doi.acm.org/10.1145/570681.570682
117. Helger Lipmaa, **N. Asokan**, Valtteri Niemi: Secure Vickrey Auctions without Threshold Trust, Financial Cryptography 2002, volume 2357 of Lecture Notes in Computer Science, pages 87-101, March, 2002. Springer-Verlag. http://dx.doi.org/10.1007/3-540-36504-4_7
118. Henry Haverinen, Tuomas Maattanen, **N. Asokan**: Authentication and Key Generation for Mobile IP Using GSM Authentication and Roaming, Proceedings of the IEEE International Conference on Communications, Pages 2453-2457, volume 8, Helsinki Finland, June 2001. http://dx.doi.org/10.1109/ICC.2001.936589
119. Philip Ginzboorg, **N. Asokan**: Key Agreement in Ad-hoc Networks, Proceedings of the NordSec '99 workshop, Kista, Sweden, November 1999.
120. **N. Asokan**, Els Van Herreweghen, Michael Steiner: Towards a Framework for Handling Disputes in Payment Systems, Proceedings of the Third Usenix Workshop on Electronic Commerce, Boston, Mass., September 1998, pages 187-202. https://www.usenix.org/conference/3rd-usenix-workshop-electronic-commerce/towards-framework-handling-disputes-payment
121. Günter Karjoth, Ceki Gülcü, **N. Asokan**: Protecting the Computation Results of Free-roaming Agents Proceedings of the Second International Workshop on Mobile Agents (MA '98), number 1477 in Lecture Notes in Computer Science, pages 195-207, Springer-Verlag, September 1998. http://dx.doi.org/10.1007/BFb005765910.1007/BF01324939

122. **N. Asokan**, Victor Shoup, Michael Waidner: Asynchronous Protocols for Optimistic Fair Exchange, Proceedings of the IEEE Symposium on Research in Security and Privacy, Oakland, CA, May 1998. IEEE Computer Society Press, pages 86-99. http://dx.doi.org/10.1109/SECPRI.1998.674826
123. **N. Asokan**, Victor Shoup, Michael Waidner: Optimistic Fair Exchange of Digital Signatures, In Kaisa Nyberg, editor, Advances in Cryptology - EUROCRYPT '98, Helsinki, Finland, June 1998, number 1403 in Lecture Notes in Computer Science, pages 591-606, Springer-Verlag, May 1998. http://dx.doi.org/10.1007/BFb0054156
124. **N. Asokan**, Matthias Schunter, Michael Waidner: Optimistic Protocols for Fair Exchange, 4th ACM Conference on Computer and Communications Security (CCS), Zurich, Switzerland, April 1997. ACM Press, pages 6, 8{17. http://doi.acm.org/10.1145/266420.266426
125. **N. Asokan**, Gene Tsudik, Michael Waidner: Server-supported Signatures, Proceedings of the Fourth European Symposium on Research in Computer Security (ESORICS), number 1146 in Lecture Notes in Computer Science, pages 131-143. Springer-Verlag, September 1996. http://dx.doi.org/10.1007/3-540-61770-1_32
126. Didier Samfat, Refik Molva, **N. Asokan**: Untraceability in Mobile Networks, Proceedings of the ACM International Conference on Mobile Computing and Networking (Mobicom), Berkeley, Nov. 1995. http://doi.acm.org/10.1145/215530.215548
127. **N. Asokan**: Anonymity in a Mobile Computing Environment, Proceedings of the Workshop on Mobile Computing Systems and Applications, Santa Cruz, Dec. 1994. http://dx.doi.org/10.1109/MCSA.1994.513484
128. **N. Asokan**, Ravi V. Shankar, Kishan Mehrotra, C. Mohan, Sanjay Ranka: A Neural Network Simulator for the Connection Machine, Proceedings of the Fifth International Symposium on Intelligent Control, 1990. http://dx.doi.org/10.1109/ISIC.1990.128506
129. **N. Asokan**, Sanjay Ranka, Ophir Frieder: A Parallel Free-text Search System with Indexing, Proceedings of the IEEE International Conference on Parallel Architectures and Databases (PARBASE), pages 519-521, March 1990. http://dx.doi.org/10.1109/PARBSE.1990
130. **N. Asokan**, Ravi V. Shankar: A Parallel Implementation of the Hough Transform Method, Proceedings of the 32nd Midwest Symposium on Circuits and Systems, Urbana-Champaign, August 1989. http://dx.doi.org/10.1109/MWSCAS.1989.101856

B Non-refereed scientific articles

B1 Non-refereed journal articles

131. **N. Asokan**: Ethics in Information Security, IEEE Security & Privacy 15(3):3-4, June 2017 (Editorial), https://doi.org/10.1109/MSP.2017.75

B2 Book section

132. **N. Asokan** et al: Architecture (Chapter 6) in SEMPER - Secure Electronic Marketplace for Europe, (edited by Gérard Lacoste et al), Springer, Lecture Notes in Computer Science 1854, pp 45-63, 2000, http://link.springer.com/content/pdf/10.1007%2F978-3-540-44927-0_8.pdf
133. **N. Asokan**, Michael Steiner: Architecture (Chapter 11) in SEMPER - Secure Electronic Marketplace for Europe, (edited by Gérard Lacoste et al), Springer, Lecture Notes in Computer Science 1854, pp 185-211, 2000, http://link.springer.com/content/pdf/10.1007%2F978-3-540-44927-0_13.pdf

B3 Non-refereed conference proceedings

134. **N. Asokan**: On Mobile malware infections. (abstract for **Invited** Talk, unrefereed), ACM Conference on Security & Privacy in Wireless and Mobile Networks, WiSec'14, pp 37-38, Oxford, United Kingdom, July 2014. http://doi.acm.org/10.1145/2627393.2627420

135. Jan-Erik Ekberg, Kari Kostiainen, **N. Asokan**: Trusted execution environments on mobile devices, Tutorial summary, ACM Conference on Computer and Communications Security, pp 1497-1498, Berlin, Germany, 2013. http://doi.acm.org/10.1145/2508859.2516758

136. **N. Asokan**, Jan-Erik Ekberg, Kari Kostiainen: The Untapped Potential of Trusted Execution Environments on Mobile Devices (abstract for **Invited** Talk, unrefereed), Financial Cryptography 2013, Okinawa, Japan, pp 293-294, Lecture Notes in Computer Science 7859, April 2013. http://link.springer.com/chapter/10.1007%2F978-3-642-39884-1_24

137. **N. Asokan**, Cynthia Kuo: Usable Mobile Security, Extended abstract accompanying **Invited** keynote; unrefereed), Proc. 8th International Conference on Distributed Computing and Internet Technology (ICDCIT 2012), Bhubaneshwar, India, February 2012. http://dx.doi.org/10.1007/978-3-642-28073-3_1

138. Kari Kostiainen, Elena Reshetova, Jan-Erik Ekberg, **N. Asokan**: Old, new, borrowed, blue: a perspective on the evolution of mobile platform security architectures (**q** paper accompanying keynote, unrefereed) In Proceedings of the First ACM Conference on Data and application security and privacy (CODASPY), San Antonio, February 2011. http://doi.acm.org/10.1145/1943513.1943517

C Scientific books (monograph)

C1 Book

139. **N. Asokan**, Lucas Davi, Alexandra Dmitrienko, Stephan Heuser, Kari Kostiainen, Elena Reshetova, Ahmad-Reza Sadeghi: Mobile Platform Security, in the series “Synthesis Lectures on Information Security, Privacy, and Trust”, Morgan & Claypool Publishers, 2014. http://dx.doi.org/10.2200/S00555ED1V01Y201312SPT009

140. Silke Holtmanns, Pekka Laitinen, Philip Ginzboorg, Valtteri Niemi, **N. Asokan**: Cellular Authentication for Mobile and Internet Services, Wiley, 2008, ISBN: 978-0-470-72317-3, http://eu.wiley.com/WileyCDA/WileyTitle/productCd-0470723173.html

C2 Edited book, conference proceedings or special issue of a journal

141. Adrienne Porter Felt, **N. Asokan**: CCS'13 co-located workshop summary for SPSM 2013. ACM Conference on Computer and Communications Security 2013: 1489-1490.

142. Michael Huth, **N. Asokan**, Srdjan Čapkun, Ivan Flechais, Lizzie Coles-Kemp (Eds.): Trust and Trustworthy Computing - 6th International Conference, TRUST 2013, London, UK, June 17-19, 2013. Proceedings. Lecture Notes in Computer Science 7904, Springer 2013, ISBN 978-3-642-38907-8

143. Dieter Gollmann, Dirk Westhoff, Gene Tsudik, **N. Asokan** (Eds.): Proceedings of the Fourth ACM Conference on Wireless Network Security, WISEC 2011, Hamburg, Germany, June 14-17, 2011. ACM 2011, ISBN 978-1-4503-0692-8

144. Shouhuai Xu, **N. Asokan**, Ahmad-Reza Sadeghi (Eds.): Proceedings of the 5th ACM Workshop on Scalable Trusted Computing, STC 2010, Chicago, Illinois, USA, October 04, 2009. ACM 2010, ISBN 978-1-4503-0095-7
145. Shouhuai Xu, **N. Asokan**, Cristina Nita-Rotaru, Jean-Pierre Seifert (Eds.): Proceedings of the 4th ACM Workshop on Scalable Trusted Computing, STC 2009, Chicago, Illinois, USA, November 13, 2009. ACM 2009, ISBN 978-1-60558-788-2

D Publications intended for professional communities

D2 Article in a professional manual or guide or professional information system,

146. Jan-Erik Ekberg, **N. Asokan**: Mobile Digital Rights Management, In Professional MITA -- Visions and Implementations, edited by Nokia, IT Press, 2002.

D3 Professional conference proceedings

147. Pekka Laitinen, Philip Ginzboorg, **N. Asokan**, Silke Holtmanns, Valtteri Niemi: Extending Cellular Authentication as a Service, First IEE International Conference on Commercialising Technology and Innovation, London, UK, September 2005. Available at http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?arnumber=1588703

D4 Published development or research report or study

148. Tommi Gröndahl, Luca Pajola, Mika Juuti, Mauro Conti, **N. Asokan**: All You Need is "Love": Evading Hate-speech Detection. CoRR abs/1808.09115 (2018), http://arxiv.org/abs/1808.09115
149. Fritz Alder, **N. Asokan**, Arseny Kurnikov, Andrew Paverd, Michael Steiner: S-FaaS: Trustworthy and Accountable Function-as-a-Service using Intel SGX. CoRR abs/1810.06080 (2018), http://arxiv.org/abs/1810.06080
150. **N. Asokan**, Thomas Nyman, Norrathep Rattanavipanon, Ahmad-Reza Sadeghi, Gene Tsudik: ASSURED: Architecture for Secure Software Update of Realistic Embedded Devices. CoRR abs/1807.05002 (2018), http://arxiv.org/abs/1807.05002
151. Lachlan J. Gunn, Ricardo Vieitez Parra, **N. Asokan**: On The Use of Remote Attestation to Break and Repair Deniability. IACR Cryptology ePrint Archive 2018: 424 (2018), https://eprint.iacr.org/2018/424
152. Mika Juuti, Sebastian Szyller, Alexey Dmitrenko, Samuel Marchal, **N. Asokan**: PRADA: Protecting against DNN Model Stealing Attacks. CoRR abs/1805.02628 (2018), http://arxiv.org/abs/1805.02628
153. Mika Juuti, Bo Sun, Tatsuya Mori, **N. Asokan**: Stay On-Topic: Generating Context-specific Fake Restaurant Reviews. CoRR abs/1805.02400 (2018), http://arxiv.org/abs/1805.02400
154. Arseny Kurnikov, Andrew Paverd, Mohammad Mannan, **N. Asokan**: Keys in the Clouds: Auditable Multi-device Access to Cryptographic Credentials. CoRR abs/1804.08569 (2018), http://arxiv.org/abs/1804.08569
155. Thien Duc Nguyen, Samuel Marchal, Markus Miettinen, Minh Hoang Dang, **N. Asokan**, Ahmad-Reza Sadeghi: DÏoT: A Crowdsourced Self-learning Approach for Detecting Compromised IoT Devices. CoRR abs/1804.07474 (2018), http://arxiv.org/abs/1804.07474

156. Hien Thi Thu Truong, Juhani Toivonen, Thien Duc Nguyen, Sasu Tarkoma, **N. Asokan**: Proximity Verification Based on Acoustic Room Impulse Response, CoRR abs/1803.07211, https://arxiv.org/abs/1803.07211
157. Fritz Alder, Arseny Kurnikov, Andrew Paverd and **N. Asokan**: Migrating SGX Enclaves with Persistent State, CoRR abs/1803.11021 (2018), https://arxiv.org/abs/1803.11021
158. Jian Liu, Duan Li, Yong Li, **N. Asokan**: Secure Deduplication of Encrypted Data: Refined Model and New Constructions, IACR Cryptology ePrint Archive 2017: 1089 (2017), http://eprint.iacr.org/2017/1089
159. Elena Reshetova, Hans Liljestrand, Andrew Paverd, **N.Asokan**: Towards Linux Kernel Memory Safety. CoRR abs/ arXiv:1710.06175 /2017, https://arxiv.org/abs/1710.06175
160. Klaudia Krawiecka, Arseny Kurnikov, Andrew Paverd, Mohammad Mannan, N. Asokan: Protecting Web Passwords from Rogue Servers using Trusted Execution Environments. CoRR abs/1709.01261 (2017), https://arxiv.org/abs/1709.01261
161. Ágnes Kiss, Jian Liu, Thomas Schneider, **N. Asokan**, Benny Pinkas: Private Set Intersection for Unequal Set Sizes with Mobile Applications, IACR ePrint Report 2017/670, https://eprint.iacr.org/2017/670
162. Jian Liu, Mika Juuti, Yao Lu, **N. Asokan**: Oblivious Neural Network Predictions via MiniONN transformationsm IACR ePrint Report 2017/452, https://eprint.iacr.org/2017/452
163. Thomas Nyman, Jan-Erik Ekberg, Lucas Davi, **N. Asokan**: CFI CaRE: Hardware-supported Call and Return Enforcement for Commercial Microcontrollers. CoRR abs/1706.05715, https://arxiv.org/abs/1706.05715
164. Ghada Dessouky, Shaza Zeitouni, Thomas Nyman, Andrew Paverd, Lucas Davi, Patrick Koeberl, **N. Asokan**, Ahmad-Reza Sadeghi: LO-FAT: Low-Overhead Control Flow ATtestation in Hardware. CoRR abs/1706.03754 (2017), https://arxiv.org/abs/1706.03754
165. Thomas Nyman, Ghada Dessouky, Shaza Zeitouni, Aaro Lehikoinen, Andrew Paverd, **N. Asokan**, Ahmad-Reza Sadeghi: HardScope: Thwarting DOP with Hardware-assisted Run-time Scope Enforcement. CoRR abs/1705.10295 (2017), https://arxiv.org/abs/1705.10295
166. Radek Tomsu, Samuel Marchal, **N. Asokan**: Profiling Users by Modeling Web Transactions. CoRR abs/1703.09745 (2017), http://arxiv.org/abs/1703.09745
167. Markus Miettinen, Samuel Marchal, Ibbad Hafeez, **N. Asokan**, Ahmad-Reza Sadeghi, Sasu Tarkoma: IoT Sentinel: Automated Device-Type Identification for Security Enforcement in IoT. CoRR abs/1611.04880 (2016), http://arxiv.org/abs/1611.04880
168. Jian Liu, Wenting Li, Ghassan O. Karame, **N. Asokan**: Scalable Byzantine Consensus via Hardware-assisted Secret Sharing. CoRR abs/1612.04997 (2016), http://arxiv.org/abs/1612.04997
169. Mika Juuti, Christian Vaas, Ivo Sluganovic, Hans Liljestrand, **N. Asokan**, Ivan Martinovic: TRec: Relay-Resilient Transparent Authentication using Trajectory Recognition. CoRR abs/1610.02801 (2016), http://arxiv.org/abs/1610.02801
170. Elena Reshetova, Filippo Bonazzi, **N. Asokan**: SELint: an SEAndroid policy analysis tool. CoRR abs/1608.02339 (2016), http://arxiv.org/abs/1608.02339

171. Jian Liu, Wenting Li, Ghassan O. Karame, **N. Asokan**: Towards Fairness of Cryptocurrency Payments. CoRR abs/1609.07256 (2016) , http://arxiv.org/abs/1609.07256

172. Tigist Abera, **N. Asokan**, Lucas Davi, Jan-Erik Ekberg, Thomas Nyman, Andrew Paverd, Ahmad-Reza Sadeghi, Gene Tsudik: C-FLAT: Control-FLow ATtestation for Embedded Systems Software. CoRR abs/1605.07763 (2016), http://arxiv.org/abs/1605.07763

173. Sandeep Tamrakar, Jian Liu, Andrew Paverd, Jan-Erik Ekberg, Benny Pinkas, **N. Asokan**: The Circle Game: Scalable Private Membership Test Using Trusted Hardware. CoRR abs/1606.01655 (2016), http://arxiv.org/abs/1606.01655

174. Sandeep Tamrakar, Long Nguyen, Praveen Kumar Pendyala, Andrew Paverd, **N. Asokan**, Ahmad-Reza Sadeghi: OmniShare: Securely Accessing Encrypted Cloud Storage from Multiple Authorized Devices, CoRR abs/1511.02119 (2015), http://arxiv.org/abs/1511.02119

175. Babins Shrestha, Nitesh Saxena, Hien Thi Thu Truong, **N. Asokan**: Contextual Proximity Detection in the Face of Context-Manipulating Adversaries, CoRR abs/1511.00905 (2015), http://arxiv.org/abs/1511.00905

176. Altaf Shaik, Ravishankar Borgaonkar, **N. Asokan**, Valtteri Niemi, Jean-Pierre Seifert: Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems, CoRR abs/1510.07563 (2015), http://arxiv.org/abs/1510.07563

177. Samuel Marchal, Kalle Saari, Nidhi Singh, **N. Asokan**: Know Your Phish: Novel Techniques for Detecting Phishing Sites and their Targets, CoRR abs/1510.07563 (2015) http://arxiv.org/abs/1510.06501

178. Thomas Nyman, Brian McGillion, **N. Asokan**: On Making Emerging Trusted Execution Environments Accessible to Developers, CoRR abs/1506.07739 (2015), http://arxiv.org/abs/1506.07739

179. Brian McGillion, Tanel Dettenborn, Thomas Nyman, **N. Asokan**: Open-TEE - An Open Virtual Trusted Execution Environment, CoRR abs/1506.07367 (2015), http://arxiv.org/abs/1506.07367

180. Otto Huhta, Prakash Shrestha, Swapnil Udar, Mika Juuti, Nitesh Saxena, **N. Asokan**: Pitfalls in Designing Zero-Effort Deauthentication: Opportunistic Human Observation Attacks, CoRR abs/1505.05779 (2015). http://arxiv.org/abs/1505.05779

181. Jian Liu, **N. Asokan** and Benny Pinkas: Secure Deduplication of Encrypted Data without Additional Independent Servers, Cryptology ePrint Archive: Report 2015/455 (2015). https://eprint.iacr.org/2015/455

182. Sourav Bhattacharya, Otto Huhta, **N. Asokan**: LookAhead: Augmenting Crowdsourced Website Reputation Systems With Predictive Modeling. CoRR abs/1504.04730 (2015). http://arxiv.org/abs/1504.04730

183. Marcin Nagy, Thanh Bui, Emiliano De Cristofaro, **N. Asokan**, Joerg Ott, Ahmad-Reza Sadeghi: How Far Removed Are You? Scalable Privacy-Preserving Estimation of Social Path Length with Social PaL, CoRR abs/1412.2433 (2014). http://arxiv.org/abs/1412.2433

184. Thomas Nyman, Jan-Erik Ekberg, **N. Asokan**: Citizen Electronic Identities using TPM 2.0. CoRR abs/1409.1023 (2014). http://arxiv.org/abs/1409.1023

185. Elena Reshetova, Janne Karhunen, Thomas Nyman, **N. Asokan**: Security of OS-level virtualization technologies: Technical report. CoRR abs/1407.4245 (2014). http://arxiv.org/abs/1407.4245
186. Hien Thi Thu Truong, Eemil Lagerspetz, Petteri Nurmi, Adam J. Oliner, Sasu Tarkoma, N. Asokan, Sourav Bhattacharya: The Company You Keep: Mobile Malware Infection Rates and Inexpensive Risk Indicators, CoRR abs/1312.3245, 2013. http://arxiv.org/abs/1312.3245
187. Markus Miettinen, Stephan Heuser, Wiebke Kronz, Ahmad-Reza Sadeghi, **N. Asokan**: ConXsense - Context Sensing for Adaptive Usable Access Control. CoRR abs/1308.2903, 2013. http://arxiv.org/abs/1308.2903
188. Marcin Nagy, Emiliano De Cristofaro, Alexandra Dmitrienko, **N. Asokan**, Ahmad-Reza Sadeghi: Do I know you? - Efficient and Privacy-Preserving Common Friend-Finder Protocols and Applications. IACR Cryptology ePrint Archive 2013: 620, 2013. http://eprint.iacr.org/2013/620
189. Marcin Nagy, **N. Asokan**, Jörg Ott: PeerShare: A System Secure Distribution of Sensitive Data Among Social Contacts, Technical Report: arXiv:1307.4046, July 2013 http://arxiv.org/abs/1307.4046
190. **N. Asokan**, Alexandra Dmitrienko, Marcin Nagy, Elena Reshetova, Ahmad-Reza Sadeghi, Thomas Schneider, Stanislaus Stelle: CrowdShare: Secure Mobile Resource Sharing , Technical Report: TU Darmstadt Technical Report TUD-CS-2013-0084, April 2013.
191. Aditi Gupta, Markus Miettinen, Marcin Nagy, **N. Asokan**, Alexandre Wetzel: Intuitive security policy configuration in mobile devices using context profiling, Technical Report: CERIAS Technical Report TR 2011-13, Purdue University, December 2011. http://www.cerias.purdue.edu/apps/reports_and_papers/view/4577
192. John Solis, Philip Ginzboorg, **N. Asokan**, Jörg Ott: Best effort authentication for opportunistic networks, Aalto University Electrical Engineering technical report. ISBN 978-952-60-4287-9, October, 2011, http://lib.tkk.fi/SCIENCE_TECHNOLOGY/2011/isbn9789526042879.pdf
193. John Solis, **N. Asokan**, Kari Kostiainen, Philip Ginzboorg, Jörg Ott: Controlling Resource Hogs in Delay-Tolerant Networks, Nokia Research Center, Technical Report NRC-TR-2008-006, July 2008. http://research.nokia.com/files/NRCTR2008006.pdf
194. Kari Kostiainen, Jan-Erik Ekberg, **N. Asokan**, Aarne Rantala: On-board Credentials with Open Provisioning, Nokia Research Center Technical Report, NRC-TR-2008-007, August 2008. http://research.nokia.com/files/NRCTR2008007.pdf
195. Jan-Erik Ekberg, **N. Asokan**, Kari Kostiainen, Pasi Eronen, Aarne Rantala, Aishvarya Sharma: OnBoard Credentials Platform Design and Implementation, Nokia Research Center Technical Report, NRC-TR-2008-001, January 2008. http://research.nokia.com/files/tr/NRC-TR-2008-001.pdf
196. Ahmad-Reza Sadeghi, Marko Wolf, Christian Stüble, **N. Asokan**, Jan-Erik Ekberg: Enabling Fairer Digital Rights Management with Trusted Computing, Horst Görtz Institute for IT Security technical report HGI-TR-2007-002, July 2007.
197. **N. Asokan**, Kari Kostiainen, Philip Ginzboorg, Jörg Ott, Cheng Luo: Towards Securing Disruption-Tolerant Networking, Nokia Research Center, Technical Report NRC-TR-2007-007, March 2007. http://research.nokia.com/files/NRCTR2007007.pdf
198. Jani Suomalainen, Jukka Valkonen, **N. Asokan** Security Associations in Personal Networks: A Comparative Analysis, Nokia Research Center, Technical Report NRC-TR-2007-004, January 2007. http://research.nokia.com/files/NRCTR2007004.pdf
199. Ersin Uzun, Kristiina Karvonen, **N. Asokan**: Usability Analysis of Secure Pairing Methods, Nokia Research Center, Technical Report NRC-TR-2007-002, January 2007. http://research.nokia.com/files/NRCTR2007002.pdf

200. Nitesh Saxena, Jan-Erik Ekberg, Kari Kostiainen, **N. Asokan**: Secure Device Pairing based on a Visual Channel, IACR ePrint Archive 2006/050. http://eprint.iacr.org/2006/050
201. Sven Laur, **N. Asokan**, Kaisa Nyberg, Efficient Mutual Data Authentication Using Manually Authenticated Strings, IACR ePrint Archive 2005/424. http://eprint.iacr.org/2005/424
202. **N. Asokan**, Kaisa Nyberg, Valtteri Niemi: Man-in-the-middle in Tunneled Authentication Protocols, IACR ePrint archive, 2002/163. http://eprint.iacr.org/2002/163/
203. **N. Asokan**, Els Van Herreweghen, Michael Steiner: Towards a Framework for Handling Disputes in Payment Systems, Research Report RZ 2996 (#93042) IBM Research, March 1998.
204. **N. Asokan**, Victor Shoup, Michael Waidner: Asynchronous Protocols for Optimistic Fair Exchange, Research Report RZ 2976 (#93022) IBM Research, November 1997. http://www.zurich.ibm.com/security/publications/1997/ASW97c.ps.gz
205. **N. Asokan**, Victor Shoup, Michael Waidner: Optimistic Fair Exchange of Digital Signatures, Research Report RZ 2973 (#93019), IBM Research, November 1997.
206. J. L. Abad-Peiro, **N. Asokan**, Michael Steiner, Michael Waidner: Designing a Generic Payment Service, Research Report RZ 2891 (# 90839), IBM Research, December 1996.
207. **N. Asokan**, Matthias Schunter, Michael Waidner: Optimistic Protocols for Multi-party Fair Exchange, Research Report RZ 2892 (# 90840), IBM Research, December 1996.
208. **N. Asokan**, Matthias Schunter, Michael Waidner: Optimistic Fair Exchange , Research Report RZ 2858, IBM Research, September 1996.
209. **N. Asokan**, Ravi Shankar, Kishan Mehrotra, C. Mohan, Sanjay Ranka: A Neural Network Simulator for the Connection Machine, Syracuse University Technical Report SU-CIS-90-10. http://surface.syr.edu/eecs_techreports/53/
210. **N. Asokan**, Sanjay Ranka, Ophir Frieder: A Parallel Free-text Search System with Indexing, Syracuse University Technical Report SU-CIS-90-1. http://surface.syr.edu/eecs_techreports/63/

D5 Textbook, professional manual or guide, dictionary

211. Contributor: Nokia and CE4A: Terminal Mode (later “MirrorLink") Technical Architecture v1.0, 2010
212. Contributor: Bluetooth Special Interest Group: Bluetooth Secure Simple Pairing specification. (included in Bluetooth 2.1 and later), 2007
213. Contributor: USB Implementors Forum: Association Models Supplement to the Certified Wireless Universal Serial Bus Specification, 2006

G Theses

G1 Polytechnic thesis, Bachelor’s thesis

214. **N. Asokan** and Pradeep Fatehpuria: A Multiprocessor Database System, Thesis for Bachelor of Technology (BTech) degree, Department of Computer Science and Engineering, Indian Institute of Technology, Kharagpur, India, May 1988.

G4 Doctoral dissertation (monograph)

215. **N. Asokan**: Fairness in Electronic Commerce, Dissertation for Doctor of Philosophy (PhD) degree, Department of Computer Science, University of Waterloo, Canada, May 1998. http://www.collectionscanada.gc.ca/obj/s4/f2/dsk2/ftp02/NQ32811.pdf

H Patents and invention disclosures

Granted Patents: (Open this link for an up-to-date list of granted US patents)

216. Method and system for byzantine fault-tolerance replicating of data on a plurality of servers (US 10,049,017)
217. Method and apparatus for accelerated authentication (US 9,979,545)
218. Method and apparatus for providing bootstrapping procedures in a communication network (US 9,906,528)
219. Method and device for verifying the integrity of platform software of an electronic device (US 9,881,150)
220. Device to device security using NAF key (US 9,781,085)
221. Mechanisms for certificate revocation status verification on constrained devices (US 9,756,036)
222. Method and apparatus for accelerated authentication (US 9,667,423)
223. Authenticating security parameters (US 9,503,462)
224. Method and device for verifying the integrity of platform software of an electronic device (US 9,438,608)
225. Method and apparatus for providing bootstrapping procedures in a communication network (US 9,300,641)
226. Implementation of an integrity-protected secure storage (US 9,171,187)
227. Method and apparatus to reset platform configuration register in mobile trusted module (US 9,087,198)
228. Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests (US 9,003,486)
229. Method and device for verifying the integrity of platform software of an electronic device (US 8,954,738)
230. Method and apparatus for adjusting context-based factors for selecting a security policy (US 8,898,793)
231. Methods, apparatuses, and computer program products for bootstrapping device and user authentication (US 8,869,252)
232. Securing communication (US 8,769,284)
233. Credential provisioning (US 8,724,819)
234. Method, apparatus and computer program product for secure software installation (US 8,701,197)
235. Method and apparatus for selecting a security policy (US 8,621,656)
236. Method and apparatus to bind a key to a namespace (US 8,566,910)
237. Administration of wireless local area networks (US 8,532,304)
238. System and method for establishing bearer-independent and secure connections (US 8,484,466)
239. Requesting digital certificates (US 8,397,060)
240. Authenticated group key agreement in groups such as ad-hoc scenarios (US 8,386,782)

241. Methods, apparatuses, and computer program products for authentication of fragments using hash trees (US 8,352,737)
242. Secure data transfer (US 8,145,907)
243. Establishment of a trusted relationship between unknown communication parties (US 8,132,005)
244. Accessing protected data on network storage from multiple devices (US 8,059,818)
245. Method and system for managing cryptographic keys (EP1561299, US 7,920,706)
246. Address acquisition. (US 6,959,009, US 7,920,575)
247. Method for remote message attestation in a communication system (US 7,913,086)
248. Authenticating users (US 7,788,493)
249. System, method and computer program product for authenticating a data agreement between network entities (US 7,783,041)
250. Linked authentication protocols (US 7,707,412)
251. Method for protecting electronic device, and electronic device (US 7,630,495)
252. System and method for dynamically enforcing digital rights management rules (US 7,529,929)
253. Information hiding non-interactive proofs-of-work (Korea 37764-KR-PCT)
254. Secure backup and recovery using a key recovery service (Korea 808654)
255. Controlling delivery of certificates in a mobile communication system (US 7,526,642)
256. Method for sharing the authorization to use specific resources (US 7,343,014)
257. System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure (US 7,308,431)
258. Method, system, and devices for transferring accounting information (US 7,251,733)
259. Method, system and computer program product for secure ticketing in a communication device (US 7,207,060)
260. Method for applying electronic payment schemes in short-range e-commerce. (US 7,194,438)
261. IP mobility in a communication system (US 7,191,226)
262. Method, system and computer program product for a trusted counter in an external security element for securing a personal communication device. (US 7,178,041)
263. Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal (US 7,149,895, EP 1026641)
264. Authentication in a packet data network. (US 7,107,620, US 7,512,796, EP1273128)
265. System and method of bootstrapping a temporary public-key infrastructure from a cellular communication authentication and billing infrastructure. (US 7,107,248, EP1397787B1)
266. Addressing and routing in mobile ad hoc networks.
267. SIM based authentication mechanism for DHCPv4/v6 messages. (US 6,704,789, EP1175765B1)

Invention disclosures: Pending patent applications are too numerous to list here in full. The complete list of patents and patent applications at the European patent office can be found here. The complete list of patent applications (70 items) at the US patent office can be found here.

Citations Record

- Google Scholar: 11,880+ citations, H-Index: 50
  http://scholar.google.com/citations?user=0MqQ8AgAAAAJ&hl=en

- Researcher ID: 990+ citations, H-Index: 13 http://www.researcherid.com/rid/D-3182-2012