Publications

Prof. N. Asokan
August 2018

A Peer-reviewed scientific articles

A1 Journal article (refereed), original research


   [http://dx.doi.org/10.1109/TIFS.2010.2096217](http://dx.doi.org/10.1109/TIFS.2010.2096217)

   [http://dx.doi.org/10.1016/j.comcom.2009.07.019](http://dx.doi.org/10.1016/j.comcom.2009.07.019)


   [http://dx.doi.org/10.1016/S0140-3664(00)00249-8](http://dx.doi.org/10.1016/S0140-3664(00)00249-8)

   [http://dx.doi.org/10.1016/S1389-1286(98)00020-6](http://dx.doi.org/10.1016/S1389-1286(98)00020-6)

   [http://dx.doi.org/10.1007/BF01324939](http://dx.doi.org/10.1007/BF01324939)

   [http://dx.doi.org/10.1109/49.839935](http://dx.doi.org/10.1109/49.839935)

   [http://dx.doi.org/10.1147/sj.371.0072](http://dx.doi.org/10.1147/sj.371.0072)

   [http://dx.doi.org/10.3233/JCS-1997-5105](http://dx.doi.org/10.3233/JCS-1997-5105)

### A2 Review article, Literature review, Systematic review


### A3 Book section, chapters in research books


A4 Conference proceedings


58. 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]


63. Thomas Nyman, Jan-Erik Ekberg, N. Asokan: Citizen Electronic Identities using TPM 2.0. ACM TrustED@CCS 2014: 37-48 [http://dx.doi.org/10.1145/2666141.2666146]


77. 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


80. 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

82. 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](http://dx.doi.org/10.1145/2046582.2046591)


84. 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](http://dx.doi.org/10.1007/978-3-642-21599-5_6)

85. 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](http://dx.doi.org/10.1007/978-3-642-21554-4_23)

86. 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](http://dx.doi.org/10.1109/PERCOM.2011.5767583)

87. 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](http://dx.doi.org/10.1007/978-3-642-25283-9_14)

88. 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](http://dx.doi.org/10.1007/978-3-642-27937-9_6)

89. 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](http://dx.doi.org/10.1007/978-3-642-27937-9_12)


92. 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](http://dx.doi.org/10.1007/978-3-642-13869-0_3)


95. 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...

   [http://doi.acm.org/10.1145/1373290.1373297](http://doi.acm.org/10.1145/1373290.1373297)

   [http://dx.doi.org/10.1007/978-3-540-85230-8_31](http://dx.doi.org/10.1007/978-3-540-85230-8_31)

   [http://doi.acm.org/10.1145/1314354.1314363](http://doi.acm.org/10.1145/1314354.1314363)

    [http://dx.doi.org/10.1007/978-3-540-75496-1_4](http://dx.doi.org/10.1007/978-3-540-75496-1_4)

    [http://doi.acm.org/10.1145/1280680.1280705](http://doi.acm.org/10.1145/1280680.1280705)

    [http://dx.doi.org/10.1145/1247694.1247705](http://dx.doi.org/10.1145/1247694.1247705)

    [http://dx.doi.org/10.1007/978-3-540-73275-4_4](http://dx.doi.org/10.1007/978-3-540-73275-4_4)

    [http://dx.doi.org/10.1007/978-3-540-77366-5_29](http://dx.doi.org/10.1007/978-3-540-77366-5_29)

    [http://dx.doi.org/10.1007/11964254_14](http://dx.doi.org/10.1007/11964254_14)

    [http://doi.ieeecomputersociety.org/10.1109/SP.2006.35](http://doi.ieeecomputersociety.org/10.1109/SP.2006.35)

    [http://dx.doi.org/10.1109/COMSWA.2006.1665195](http://dx.doi.org/10.1109/COMSWA.2006.1665195)


Publications of Prof. N. Asokan  August 2018


B Non-refereed scientific articles

B1 Non-refereed journal articles


B2 Book section


B3 Non-refereed conference proceedings


134. 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


C Scientific books (monograph)

C1 Book


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


**D Publications intended for professional communities**

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


**D3 Professional conference proceedings**


**D4 Published development or research report or study**


  http://arxiv.org/abs/1510.06501

  http://arxiv.org/abs/1506.07739

  http://arxiv.org/abs/1506.07367

  http://arxiv.org/abs/1505.05779

  https://eprint.iacr.org/2015/455

  http://arxiv.org/abs/1504.04730


   http://surface.syr.edu/eecs_techreports/53/

   http://surface.syr.edu/eecs_techreports/63/

D5 Textbook, professional manual or guide, dictionary


207. Contributor: Bluetooth Special Interest Group: Bluetooth Secure Simple Pairing specification. (included in Bluetooth 2.1 and later), 2007


G Theses

G1 Polytechnic thesis, Bachelor’s thesis


G4 Doctoral dissertation (monograph)


H Patents and invention disclosures

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

211. Method and apparatus for accelerated authentication (US 9,979,545)
| 212. | Method and apparatus for providing bootstrapping procedures in a communication network (US 9,906,528) |
| 213. | Method and device for verifying the integrity of platform software of an electronic device (US 9,881,150) |
| 214. | Device to device security using NAF key (US 9,781,085) |
| 215. | Mechanisms for certificate revocation status verification on constrained devices (US 9,756,036) |
| 216. | Method and apparatus for accelerated authentication (US 9,667,423) |
| 217. | Authenticating security parameters (US 9,503,462) |
| 218. | Method and device for verifying the integrity of platform software of an electronic device (US 9,438,608) |
| 219. | Method and apparatus for providing bootstrapping procedures in a communication network (US 9,300,641) |
| 220. | Implementation of an integrity-protected secure storage (US 9,171,187) |
| 221. | Method and apparatus to reset platform configuration register in mobile trusted module (US 9,087,198) |
| 222. | Methods and apparatus for reliable and privacy protecting identification of parties' mutual friends and common interests (US 9,003,486) |
| 223. | Method and device for verifying the integrity of platform software of an electronic device (US 8,954,738) |
| 224. | Method and apparatus for adjusting context-based factors for selecting a security policy (US 8,898,793) |
| 225. | Methods, apparatuses, and computer program products for bootstrapping device and user authentication (US 8,869,252) |
| 226. | Securing communication (US 8,769,284) |
| 227. | Credential provisioning (US 8,724,819) |
| 228. | Method, apparatus and computer program product for secure software installation (US 8,701,197) |
| 229. | Method and apparatus for selecting a security policy (US 8,621,656) |
| 230. | Method and apparatus to bind a key to a namespace (US 8,566,910) |
| 231. | Administration of wireless local area networks (US 8,532,304) |
| 232. | System and method for establishing bearer-independent and secure connections (US 8,484,466) |
| 233. | Requesting digital certificates (US 8,397,060) |
| 234. | Authenticated group key agreement in groups such as ad-hoc scenarios (US 8,386,782) |
| 235. | Methods, apparatuses, and computer program products for authentication of fragments using hash trees (US 8,352,737) |
| 236. | Secure data transfer (US 8,145,907) |
| 237. | Establishment of a trusted relationship between unknown communication parties (US 8,132,005) |
| 238. | Accessing protected data on network storage from multiple devices (US 8,059,818) |
| 239. | Method and system for managing cryptographic keys (EP1561299, US 7,920,706) |
| 240. | Address acquisition. (US 6,959,009, US 7,920,575) |
| 241. | Method for remote message attestation in a communication system (US 7,913,086) |
| 242. | Authenticating users (US 7,788,493) |
| 243. | System, method and computer program product for authenticating a data agreement between network entities (US 7,783,041) |
| 244. | Linked authentication protocols (US 7,707,412) |
245. Method for protecting electronic device, and electronic device (US 7,630,495)
246. System and method for dynamically enforcing digital rights management rules (US 7,529,929)
247. Information hiding non-interactive proofs-of-work (Korea 37764-KR-PCT)
248. Secure backup and recovery using a key recovery service (Korea 808654)
249. Controlling delivery of certificates in a mobile communication system (US 7,526,642)
250. Method for sharing the authorization to use specific resources (US 7,343,014)
251. System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure (US 7,308,431)
252. Method, system, and devices for transferring accounting information (US 7,251,733)
253. Method, system and computer program product for secure ticketing in a communication device (US 7,207,060)
254. Method for applying electronic payment schemes in short-range e-commerce. (US 7,194,438)
255. IP mobility in a communication system (US 7,191,226)
256. 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)
257. Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal (US 7,149,895, EP 1026641)
261. 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 pending patent applications (50 items) at the US patent office can be found [here](#).

Citations Record

- Google Scholar: 11,610+ citations, H-Index: 50
  [http://scholar.google.com/citations?user=0MqQ8AgAAAAJ&hl=en](http://scholar.google.com/citations?user=0MqQ8AgAAAAJ&hl=en)