A Peer-reviewed scientific articles

A1 Journal article (refereed), original research

https://doi.org/10.1002/spe.2638


   https://www.usenix.org/conference/usenixsecurity23/presentation/vyas
https://doi.org/10.1145/3338466.3358916
https://www.usenix.org/conference/usenixsecurity19/presentation/liljestrand
61. 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
https://doi.org/10.1109/EuroSP.2018.00022
68. 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


94. 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


113. 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


http://dx.doi.org/10.1007/978-3-642-25283-9_14

http://dx.doi.org/10.1007/978-3-642-27937-9_6

http://dx.doi.org/10.1007/978-3-642-27937-9_12

http://doi.acm.org/10.1145/1866423.1866428

http://doi.acm.org/10.1145/1837110.1837114

http://dx.doi.org/10.1007/978-3-642-13869-0_3

http://dx.doi.org/10.1007/978-3-642-14597-1_2

http://doi.acm.org/10.1145/1533057.1533074

http://doi.acm.org/10.1145/1456455.1456465

http://www.usenix.org/events/upsec08/tech/full_papers/heiner/heiner.pdf

http://doi.acm.org/10.1145/1373290.1373297

http://dx.doi.org/10.1007/978-3-540-85230-8_31

http://doi.acm.org/10.1145/1314354.1314363

http://dx.doi.org/10.1007/978-3-540-75496-1_4


B Non-refereed scientific articles

B1 Non-refereed journal articles


B2 Book section


B3 Non-refereed conference proceedings


174. 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

175. 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
http://doi.acm.org/10.1145/1943513.1943517

C Scientific books (monograph)

C1 Book

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

D Publications intended for professional communities

D3 Professional conference proceedings


D4 Published development or research report or study


D5 Textbook, professional manual or guide, dictionary


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 patents)

1. Method and device for verifying the integrity of platform software of an electronic device (US 11,126,710)
2. Method and system for byzantine fault-tolerance replicating of data (US 10,797,877)
3. Method and system for byzantine fault-tolerance replicating of data on a plurality of servers (US 10,664,353)
4. Implementation of an integrity-protected secure storage (US 10,565,400)
5. Method and device for verifying the integrity of platform software of an electronic device (US 10,482,238, 11,126,710)
6. Method and apparatus for identity based ticketing (US 10,374,799)
7. Method and system for byzantine fault-tolerance replicating of data on a plurality of servers (US 10,049,017)
<table>
<thead>
<tr>
<th></th>
<th>Title</th>
<th>Patent Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.</td>
<td>Method and apparatus for accelerated authentication</td>
<td>US 9,979,545</td>
</tr>
<tr>
<td>9.</td>
<td>Method and apparatus for providing bootstrapping procedures in a communication network</td>
<td>US 9,906,528</td>
</tr>
<tr>
<td>10.</td>
<td>Method and device for verifying the integrity of platform software of an electronic device</td>
<td>US 9,881,150</td>
</tr>
<tr>
<td>11.</td>
<td>Device to device security using NAF key</td>
<td>US 9,781,085</td>
</tr>
<tr>
<td>12.</td>
<td>Mechanisms for certificate revocation status verification on constrained devices</td>
<td>US 9,756,036</td>
</tr>
<tr>
<td>14.</td>
<td>Authenticating security parameters</td>
<td>US 9,503,462</td>
</tr>
<tr>
<td>15.</td>
<td>Method and device for verifying the integrity of platform software of an electronic device</td>
<td>US 9,438,608</td>
</tr>
<tr>
<td>16.</td>
<td>Method and apparatus for providing bootstrapping procedures in a communication network</td>
<td>US 9,300,641</td>
</tr>
<tr>
<td>17.</td>
<td>Implementation of an integrity-protected secure storage</td>
<td>US 9,171,187</td>
</tr>
<tr>
<td>18.</td>
<td>Method and apparatus to reset platform configuration register in mobile trusted module</td>
<td>US 9,087,198</td>
</tr>
<tr>
<td>19.</td>
<td>Methods and apparatus for reliable and privacy protecting identification of parties' mutual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>friends and common interests</td>
<td>US 9,003,486</td>
</tr>
<tr>
<td>20.</td>
<td>Method and device for verifying the integrity of platform software of an electronic device</td>
<td>US 8,954,738</td>
</tr>
<tr>
<td>21.</td>
<td>Method and apparatus for adjusting context-based factors for selecting a security policy</td>
<td>US 8,898,793</td>
</tr>
<tr>
<td>22.</td>
<td>Methods, apparatuses, and computer program products for bootstrapping device and user</td>
<td>US 8,869,252</td>
</tr>
<tr>
<td></td>
<td>authentication</td>
<td></td>
</tr>
<tr>
<td>23.</td>
<td>Securing communication</td>
<td>US 8,769,284</td>
</tr>
<tr>
<td>24.</td>
<td>Credential provisioning</td>
<td>US 8,724,819</td>
</tr>
<tr>
<td>25.</td>
<td>Method, apparatus and computer program product for secure software installation</td>
<td>US 8,701,197</td>
</tr>
<tr>
<td>26.</td>
<td>Method and apparatus for selecting a security policy</td>
<td>US 8,621,656</td>
</tr>
<tr>
<td>27.</td>
<td>Method and apparatus to bind a key to a namespace</td>
<td>US 8,566,910</td>
</tr>
<tr>
<td>28.</td>
<td>Administration of wireless local area networks</td>
<td>US 8,532,304</td>
</tr>
<tr>
<td>29.</td>
<td>System and method for establishing bearer-independent and secure connections</td>
<td>US 8,484,466</td>
</tr>
<tr>
<td>30.</td>
<td>Requesting digital certificates</td>
<td>US 8,397,060</td>
</tr>
<tr>
<td>31.</td>
<td>Authenticated group key agreement in groups such as ad-hoc scenarios</td>
<td>US 8,386,782</td>
</tr>
<tr>
<td>32.</td>
<td>Methods, apparatuses, and computer program products for authentication of fragments using</td>
<td>US 8,352,737</td>
</tr>
<tr>
<td></td>
<td>hash trees</td>
<td></td>
</tr>
<tr>
<td>33.</td>
<td>Secure data transfer</td>
<td>US 8,145,907</td>
</tr>
<tr>
<td>34.</td>
<td>Establishment of a trusted relationship between unknown communication parties</td>
<td>US 8,132,005</td>
</tr>
<tr>
<td>35.</td>
<td>Accessing protected data on network storage from multiple devices</td>
<td>US 8,059,818</td>
</tr>
<tr>
<td>37.</td>
<td>Address acquisition</td>
<td>US 6,959,009, US 7,920,575</td>
</tr>
<tr>
<td>38.</td>
<td>Method for remote message attestation in a communication system</td>
<td>US 7,913,086</td>
</tr>
<tr>
<td>39.</td>
<td>Authenticating users</td>
<td>US 7,788,493</td>
</tr>
<tr>
<td>40.</td>
<td>System, method and computer program product for authenticating a data agreement between</td>
<td>US 7,783,041</td>
</tr>
<tr>
<td></td>
<td>network entities</td>
<td></td>
</tr>
<tr>
<td>41.</td>
<td>Linked authentication protocols</td>
<td>US 7,707,412</td>
</tr>
</tbody>
</table>
42. Method for protecting electronic device, and electronic device (US 7,630,495)
43. System and method for dynamically enforcing digital rights management rules (US 7,529,929)
44. Information hiding non-interactive proofs-of-work (Korea 37764-KR-PCT)
45. Secure backup and recovery using a key recovery service (Korea 808654)
46. Controlling delivery of certificates in a mobile communication system (US 7,526,642)
47. Method for sharing the authorization to use specific resources (US 7,343,014)
48. System and method of secure authentication and billing for goods and services using a cellular telecommunication and an authorization infrastructure (US 7,308,431)
49. Method, system, and devices for transferring accounting information (US 7,251,733)
50. Method, system and computer program product for secure ticketing in a communication device (US 7,207,060)
51. Method for applying electronic payment schemes in short-range e-commerce. (US 7,194,438)
52. IP mobility in a communication system (US 7,191,226)
53. 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)
54. Personal device, terminal, server and methods for establishing a trustworthy connection between a user and a terminal (US 7,149,895, EP 1026641)
57. Addressing and routing in mobile ad hoc networks.
58. SIM based authentication mechanism for DHCPv4/v6 messages. (US 6,704,789, EP1175765B1)

**Invention disclosures:** Here is a list of my [granted patents](#) and [pending patent applications](#) (according to Google Patents).

### Citations Record
- Google Scholar: 20 500+ citations, H-Index: 71
  [http://scholar.google.com/citations?user=0MqQ8AgAAAAJ&hl=en](http://scholar.google.com/citations?user=0MqQ8AgAAAAJ&hl=en)
- Web of Science (Publons/Researcher ID): 3400+ citations, H-Index: 31
  [https://www.webofscience.com/wos/author/record/150583](https://www.webofscience.com/wos/author/record/150583)
- ACM author profile [https://dl.acm.org/profile/81100611941](https://dl.acm.org/profile/81100611941)
- ORCID profile [https://orcid.org/0000-0002-5093-9871](https://orcid.org/0000-0002-5093-9871)
- Amazon author page [https://amazon.com/author/asokan](https://amazon.com/author/asokan)