Publications co-authored by Ioana Boureanu

2021/2022

A. Radu, T. Chothia, C. Newton, L. Chen, "Practical EMV Relay Protection", at the 2022 IEEE Symposium on Security and Privacy (IEEE S & P, 2022), see more here

I. Boureanu, C. Dragan, F. Dupressoir, D. Gerault, P. Lafourcade, "Precise and Mechanised Models and Proofs for Distance-Bounding", at the 34th IEEE Computer Security Foundations Symposium (CSF 2021)

2020

I. Boureanu, T. Chothia, A. Debant, S. Delaune, "Security Analysis and Implementation of Relay-Resistant Contactless Payments", at the 27th ACM Conference on Computer and Communications Security (ACM CCS 2020)

I. Boureanu, D. Migault, S. Preda, H. Alamedine, S. Mishra, F. Fieau, M. Mannan, "LURK: Server-Controlled TLS Delegation" , at the 19th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (IEEE Trustcomm 2020), Track: Security Track

S. Wesemeyer, I. Boureanu, Z. Smith, H. Treharne, "Extensive Security Verification of LoRaWAN Key Establishment: Insecurities and Patches", at the 5th IEEE European Symposium on Security and Privacy (IEEE Euro S & P 2020)

I. Boureanu, S. Ivey, L. Chen, "Provable-Security Model for Strong Proximity-based Attacks: With Application to Contactless Payments", at the 15th ACM Asia Conference on Computer and Communications Security (ACM ASIACCS 2020)

G. Avoine, I. Boureanu, D. Gérault, G. P. Hancke, P. Lafourcade, C. Onete, book-chapter "From Relay Attacks to Distance Bounding Protocols", in book "Security of Ubiquitous Computing Systems", editors Gildas Avoine, Julio Hernandez-Castro, Springer

2019

I. Boureanu, D. Gerault, J. Lewis, "Here and there at once with my mobile phone", at the 16th International Conference on Security and Cryptography (Secrypt 2019), July 2019

D. Gerault and I. Boureanu, "Distance Bounding Under Different Assumptions", at the 12th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2019), May 2019

F. Belardinelli, I. Boureanu, C. Dima, V. Malvone, "Verifying Strategic Abilities in Multi-agent Systems with Private Data-Sharing" (Extended Abstract), at the International Conference on Autonomous Agents and Multiagent Systems 2019 (AAMAS 2019), May 2019

T. Chothia, I. Boureanu, L. Chen, "Making Contactless EMV Payments Robust Against Rogue Readers Colluding With Relay Attackers", at the 23rd International Conference on Financial Cryptography and Data Security (Financial Crypto 2019), Feb. 2019, paper available here

2018

G. Avoine, M. A. Bingoel, I. Boureanu, S. Capkun, G. Hancke, S. Kardas, C. Kim, C. Lauradoux, B. Martin, J. Munilla, A. Peinado-Dominguez, K. Bonne Rasmussen, D. Singelee, A. Tchamkerten, R. Trujillo-Rasua, S.Vaudenay, "Security of Distance-Bounding: A Survey," ACM Computing Surveys, vol. 51, issue 5, 2018

K. Bhargavan, I. Boureanu, P.A. Fouque, C. Onete and A. Delignat-Lavaud, "A Formal Treatment of Accountable Proxying over TLS", at the 39th IEEE Symposium on Security and Privacy (S & P) 2018, May 2018, full version here

F. Belardinelli, I. Boureanu, C. Dima and V. Malvone,"Towards the Verification of Strategic Ability in MAS with Private Data-Sharing", at the ACTIONS (Reasoning about Actions and Processes: Highlights of Recent Advances) Workshop, affiliated with KR (Knowledge Representation) 2018

I. Boureanu and A. Anda, "Another Look at Relay and Distance-based Attacks in Contactless Payments", Cryptology ePrint Archive: Report 2018/402, May 2018

I. Boureanu, D. Gerault, P. Lafourcade, "Fine-Grained and Application-Ready Distance-Bounding Security", Cryptology ePrint Archive: Report 2018/384, May 2018

2017

I. Boureanu, D. Gerault, P. Lafourcade, C. Onete, "Breaking and Fixing the HB+DB protocol", WiSec 2017, July 2017

N. Giorgiannis, F. Raimondi, I. Boureanu, "A Novel Symbolic Approach to Verifying Epistemic Properties of Programs", IJCAI 2017, August 2017

K. Bhargavan, I. Boureanu, P.A. Fouque, C. Onete and B. Richard, "Content delivery over TLS: a cryptographic analysis of Keyless SSL", at the 2nd IEEE European Symposium on Security and Privacy (Euro S & P) 2017, April 2017

2016

I. Boureanu, P. Kouvaros , A. Lomuscio, "Verifying Security Properties in Unbounded Multiagent Systems", 15th International Conference on Autonomous Agents and Multi-Agent systems (AAMAS), May, 2016, Singapore

2015

I. Boureanu, M. Ohkubo, S. Vaudenay, "The Limits of Composable Crypto with Transferrable Setup Devices", the 10th ACM Symposium on Information, Computer and Communications Security (ASIACCS'15), April 14-17, 2015, Singapore

I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Practical & Provably Secure Distance-Bounding", Journal of Computer Security, volume 23, pages 229 --257, 2015

I. Boureanu, S. Vaudenay, "Challenges in Distance-Bounding", IEEE Security & Privacy, vol. 13, p. 41 -- 48, 2015

2014

I. Boureanu, S. Vaudenay, "Optimal Proximity Proofs", the 10th International Conference on Information Security and Cryptology (INSCRYPT 2014), December 13 - 15, pp. 170-190, 2014, Beijing, China

I. Boureanu, S. Vaudenay, "Compact and Efficient UC Commitments under Atomic-Exchanges", the 17th Annual International Conference on Information Security and Cryptology (ICISC 2014), December 3 - 5, 2014, Seoul, South Korea

I. Boureanu, P. Owesarski, S.Vaudenay, "Applied Cryptography and Network Security - 12th International Conference", Proceedings. Lecture Notes in Computer Science 8479, Springer 2014

2013

I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Practical & Provably Secure Distance-Boundings", at the 16th Information Security Conference (ISC), November 13 -- November 15, 2013, Dallas, US

I. Boureanu, S. Vaudenay, "Input-Aware Equivocable Commitments and UC-secure Commitments With Atomic Exchanges", at the 7th International Conference on Provable Security (ProvSec), October 23 - 25, 2013, Melaka, Malaysia

S. Bogos, I. Boureanu, S. Vaudenay, "Primeless Factoring-Based Cryptography : Solving the Complexity Bottleneck of Public-Key Generation", at the 11th International Conference on Applied Cryptography and Network Security (ACNS 2013), June 25 - 28, 2013, Banff, Canada

I. Boureanu, S. Vaudenay, "UC and EUC Weak Bit-Commitments Using Seal-Once Tamper-Evidence", Scientific Annals of Cuza University, vol. 23 (2), pp. 23, 2013

I. Boureanu, A Mitrokotsa, S Vaudenay, "Towards Secure Distance Bounding", the 20th anniversary annual Fast Software Encryption (FSE), March 10 - 13, 2013, Singapore

I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Secure & Lightweight Distance-Bounding", the 2nd International Workshop on Lightweight Cryptography for Security & Privacy (LightSec), May 6 - 7, 2013 Gebze, Turkey

I. Boureanu, A. Mitrokotsa, S. Vaudenay, "Practical and Provably Secure Distance-Bounding", IACR Cryptology ePrint Archive: 465, 2013

2012

I. Boureanu, A. Mitrokotsa, S. Vaudenay, "On the Pseudorandom Function Assumption in (Secure) Distance-Bounding Protocols", at the Second International Conference on Cryptology and Information Security in Latin America (LATINCRYPT), October 7 - 10, 2012, Santiago, Chile

S. Bogos, I. Boureanu, S. Vaudenay, "Primeless Modular Cryptography", at Yet Another Conference on Cryptography (YACC), September 24 - 28, 2012, Porquerolles Island, France

I. Boureanu, S. Vaudenay, "Several weak bit-commitments using seal-once tamper-evident devices", at the 6th International Conference on Provable Security (ProvSec), September 26 - 28, 2012, Chengdu, China

A. Bay, I. Boureanu, K. Mitrokotsa, I. Spulber, S. Vaudenay, "The Bussard-Bagga and Other Distance Bounding Protocols under Attack", at the 8th International Conference on Information Security and Cryptology (Inscrypt), November 28 - December 1, 2012, Beijing, China

I. Boureanu, A. Jones, A. Lomuscio, "Automatic Verification of Temporal-Epistemic Logic under Convergent Equational Theories", in Proceedings of the 11th International Conference on Autonomous Agents and Multi- Agent systems (AAMAS), June 4 - 8, 2012, Valencia, Spain

I. Boureanu, S. Vaudenay, "Several Weak Bit-Commitments Using Seal-Once Tamper-Evident Devices", IACR Cryptology ePrint Archive: 380, 2012

2010

I. Boureanu, A. Lomuscio, M. Cohen, "Model Checking Detectability of Attacks in Multiagent Systems", Proceedings of the 9th International Conference on Autonomous Agents and Multi-Agent systems (AAMAS), May 10 - 14, 2010, Toronto, Canada

2009

I. Boureanu, M. Cohen, A. Lomuscio, "Automatic Verification of Temporal-Epistemic Properties of Cryptographic Protocols", Journal of Applied Non-Classical Logics, vol 19/4, pp. 463 - 487, 2009

I. Boureanu, M. Cohen, A. Lomuscio, "A Compilation Method for the Verification of Temporal-Epistemic Properties of Cryptographic Protocols", in the Informal Proceedings of the International Workshop on Automated Reasoning for Security Protocols Analysis and Issues in the Theory of Security (ARSPA-WITS), March 28 - 29, 2009, York, UK

2008

F. Tiplea, C. Barjoveanu, C. Enea, I. Boureanu, "Secrecy for Bounded Protocols With Freshness Check is NEXPTIME-complete", Journal of Computer Security, vol.16/6, pp. 689-712, 2008

2005

S. Iftene, I. Boureanu, "Weighted Threshold Secret Sharing Based on the Chinese Remainder Theorem", Scientific Annals of Cuza University, vol. 15, pp. 161-172, 2005