Bogdan Groza

Authors:
Add personal information

Affiliation history
· Polytechnic University of Timisoara

Bibliometrics: publication history

Average citations per article	0.65
Citation Count	17
Publication count	26
Publication years	2005-2015
Available for download	3
Average downloads per article	135.33
Downloads (cumulative)	406
Downloads (12 Months)	124
Downloads (6 Weeks)	34

28 results found

Export Results: bibtex | endnote | acmref | csv

Result 1 – 20 of 28

Result page: **1** 2

Sort by: publication date

1 LiBrA-CAN: Lightweight Broadcast Authentication for Controller Area Networks

Bogdan Groza, Stefan Murvay, Anthony Van Herrewege, Ingrid Verbauwhede

April 2017 ACM Transactions on Embedded Computing Systems (TECS): Volume 16 Issue 3, May 2017

Publisher: ACM

Bibliometrics:

Citation Count: 0
Downloads (6 Weeks): 21, Downloads (12 Months): 45, Downloads (Overall): 45

Full text available: PDF

Despite realistic concerns, security is still absent from vehicular buses such as the widely used Controller Area Network (CAN). We design an efficient protocol based on efficient symmetric primitives, taking advantage of two innovative procedures: splitting keys between nodes and mixing authentication tags. This results in a higher security level ...

Keywords: CAN bus, broadcast, authentication, cryptography

2 Evaluating SRAM as Source for Fingerprints and Randomness on Automotive Grade Controllers

Bogdan Groza, Pal-Stefan Murvay, Tudor Andreica

July 2016 ICETE 2016: Proceedings of the 13th International Joint Conference on e-Business and Telecommunications

Publisher: SCITEPRESS - Science and Technology Publications, Lda

Bibliometrics:

Citation Count: 0

It is well known that the state of uninitialized SRAM provides a unique pattern on each device due to physical imperfections. Both the affinity toward some fixed state as well as the deviation from it can be successfully exploited in security mechanisms. Fixed values provide an efficient mechanism for physical ...

Keywords: Randomness, Physical Fingerprinting, SRAM.

3 Performance analysis of broadcast authentication protocols on CAN-FD and FlexRay

Paula Vasile, Bogdan Groza, Stefan Murvay

October 2015 WESS'15: Proceedings of the WESS'15: Workshop on Embedded Systems Security

Publisher: ACM

Bibliometrics:

Citation Count: 0
Downloads (6 Weeks): 3, Downloads (12 Months): 39, Downloads (Overall): 78

Full text available: PDF

In the light of the numerous reported attacks, designing cryptographic protocols for in-vehicle embedded networks was a constant preoccupation in the past few years. While several research proposals appeared, a concrete performance analysis of such protocols over a realistic network configuration is still absent from the literature. In this work ...

Keywords: broadcast authentication, FlexRay, embedded networks, CAN-FD

4 Cryptographic puzzles and DoS resilience, revisited

Bogdan Groza, Bogdan Warinschi

October 2014 Designs, Codes and Cryptography: Volume 73 Issue 1, October 2014

Publisher: Kluwer Academic Publishers

Bibliometrics:

Citation Count: 2

Cryptographic puzzles (or client puzzles) are moderately difficult problems that can be solved by investing non-trivial amounts of computation and/or storage. Devising models for cryptographic puzzles has only recently started to receive attention from the cryptographic community as a first step toward rigorous models and proofs of security of applications ...

Keywords: DoS resilience, Client puzzle, PoW protocols, 94A60

5 Performance Evaluation of SHA-2 Standard vs. SHA-3 Finalists on Two Freescale Platforms

Pal-Stefan Murvay, Bogdan Groza

October 2013 International Journal of Secure Software Engineering: Volume 4 Issue 4, October 2013

Publisher: IGI Global

Bibliometrics:

Citation Count: 0

Embedded devices are ubiquitously involved in a large variety of security applications which heavily rely on the computation of hash functions. Roughly, two alternatives for speeding up computations co-exist in these resource constrained devices: parallel processing and hardware acceleration. Needles to say, multi-core devices are clearly the next step in ...

Keywords: Parallelism, SHA-2, SHA-3, Hash Function, Coprocessor

6 Secure Broadcast with One-Time Signatures in Controller Area Networks

Bogdan Groza, Pal-Stefan Murvay

July 2013 International Journal of Mobile Computing and Multimedia Communications: Volume 5 Issue 3, July 2013

Publisher: IGI Global

Bibliometrics:

Citation Count: 0

Broadcast authentication in Controller Area Networks CAN is subject to real time constraints that are hard to satisfy by expensive public key primitives. For this purpose the authors study here the use of one-time signatures which can be built on the most computationally efficient one-way functions. The authors use an ...

Keywords: Broadcast, Controller Area Networks CAN, One-Time Signatures, S12, Authentication

7 SAPHE: simple accelerometer based wireless pairing with heuristic trees

Bogdan Groza, Rene Mayrhofer

December 2012 MoMM '12: Proceedings of the 10th International Conference on Advances in Mobile Computing & Multimedia

Publisher: ACM

Bibliometrics:

Citation Count: 4
Downloads (6 Weeks): 8, Downloads (12 Months): 23, Downloads (Overall): 113

Full text available: PDF

Accelerometers provide a good source of entropy for bootstrapping a secure communication channel in autonomous and spontaneous interactions between mobile devices that share a common context but were not previously associated. We propose two simple and efficient key exchange protocols based on accelerometer data that use only simple hash functions ...

Keywords: accelerometer, authentication, key-exchange

8 Revisiting difficulty notions for client puzzles and dos resilience

Bogdan Groza, Bogdan Warinschi

September 2012 ISC'12: Proceedings of the 15th international conference on Information Security

Publisher: Springer-Verlag

Bibliometrics:

Citation Count: 2

Cryptographic puzzles are moderately difficult problems that can be solved by investing non-trivial amounts of computation and/or storage. Devising models for cryptographic puzzles has only recently started to receive attention from the cryptographic community as a first step towards rigorous models and proofs of security of applications that employ them ...

9 Provable Synthetic Coordinates for Increasing PoWs Effectiveness against DoS and Spam

Marius Cristea, Bogdan Groza

September 2012 SOCIALCOM-PASSAT '12: Proceedings of the 2012 ASE/IEEE International Conference on Social Computing and 2012 ASE/IEEE International Conference on Privacy, Security, Risk and Trust

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

The effectiveness of synthetic coordinate systems against DoS and spam stems from the fact that, while changing or hiding a logical address is easier, changing the location of the spammer inside the network should be harder. But synthetic coordinate systems are limited by the fact that malicious nodes can easily ...

Keywords: DoS, localization, spam, Vivaldi

10 Performance improvements for SHA-3 finalists by exploiting microcontroller on-chip parallelism

Pal-Stefan Murvay, B. Groza

September 2011 CRISIS '11: Proceedings of the 2011 6th International Conference on Risks and Security of Internet and Systems (CRiSIS)

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 1

As ubiquitous devices, microcontrollers are deployed in a great variety of applications many of which involve communication over insecure channels that require cryptography. Here we investigate the possibility of using on-chip coprocessors from currently available microcontrollers for increasing computational power by employing parallelism. For this we focus on the analysis ...

Keywords: onchip coprocessors, SHA-3 finalists, ubiquitous devices, insecure communication channel, cryptography, feature identification, Freescale S12X family microcontroller, XGATE coprocessor, software implementation, BLAKE, microcontroller onchip parallelism

11 Secure Broadcast with One-Time Signatures in Controller Area Networks

Bogdan Groza, Stefan Murvay

August 2011 ARES '11: Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 1

We use one-time signatures to assure authenticity for messages that are broadcast over a Controller Area Network (CAN). The advantage is that we can use the simplest one-way functions which are computationally efficient while authentication does not depend on disclosure delays as in the case of protocols based on one-way ...

Keywords: one-time signature, broadcast authentication, CAN

12 Some Security Issues in SCALANCE Wireless Industrial Networks

Marius Cristea, Bogdan Groza, Mihai Iacob

August 2011 ARES '11: Proceedings of the 2011 Sixth International Conference on Availability, Reliability and Security

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

We discuss some security weaknesses of Scalance wireless access points and clients. These devices, developed by Siemens, are commonly used for wireless communication in network control systems. After the identification of the Stuxnet worm, which targeted PLCs from uranium enrichment facilities in Iran, these devices become of increased interest to ...

Keywords: wireless security, control system, authentication

13 Formal modelling and automatic detection of resource exhaustion attacks

Bogdan Groza, Marius Minea

March 2011 ASIACCS '11: Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security

Publisher: ACM

Bibliometrics:

Citation Count: 4
Downloads (6 Weeks): 3, Downloads (12 Months): 16, Downloads (Overall): 168

Full text available: PDF

Many common protocols: TCP, IPSec, etc., are vulnerable to denial of service attacks, where adversaries maliciously consume significant resources of honest principals, leading to resource exhaustion. We propose a set of cost-based rules that formalize DoS attacks by resource exhaustion and can automate their detection. Our classification separates excessive but ...

Keywords: automated verification, denial of service, formal modeling

14 Customizing protocol specifications for detecting resource exhaustion and guessing attacks

Bogdan Groza, Marius Minea

November 2010 FMCO'10: Proceedings of the 9th international conference on Formal Methods for Components and Objects

Publisher: Springer-Verlag

Bibliometrics:

Citation Count: 0

Model checkers for security protocols often focus on basic properties, such as confidentiality or authentication, using a standard model of the Dolev-Yao intruder. In this paper, we explore how to model other attacks, notably guessing of secrets and denial of service by resource exhaustion, using the AVANTSSAR platform with its ...

15 A formal approach for automated reasoning about off-line and undetectable on-line guessing

Bogdan Groza, Marius Minea

January 2010 FC'10: Proceedings of the 14th international conference on Financial Cryptography and Data Security

Publisher: Springer-Verlag

Bibliometrics:

Citation Count: 1

Starting from algebraic properties that enable guessing low-entropy secrets, we formalize guessing rules for symbolic verification. The rules are suited for both off-line and on-line guessing and can distinguish between them. We add our guessing rules as state transitions to protocol models that are input to model checking tools. With ...

16 A Calculus to Detect Guessing Attacks

Bogdan Groza, Marius Minea

September 2009 ISC '09: Proceedings of the 12th International Conference on Information Security

Publisher: Springer-Verlag

Bibliometrics:

Citation Count: 2

We present a calculus for detecting guessing attacks, based on oracles that instantiate cryptographic functions. Adversaries can observe oracles, or control them either on-line or off-line. These relations can be established by protocol analysis in the presence of a Dolev-Yao intruder, and the derived guessing rules can be used together ...

17 Analysis of a Password Strengthening Technique and Its Practical Use

Bogdan Groza

June 2009 SECURWARE '09: Proceedings of the 2009 Third International Conference on Emerging Security Information, Systems and Technologies

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

Besides commonly used password strengthening techniques such as salting or repeated applications of a one-way function on the password, we account a less common procedure: the truncation of the output from a one-way function on the password. This technique is used in a Norwegian ATM and a similar method is ...

Keywords: authentication, password, protocol

18 Towards Developing Secure Video Surveillance Systems over IP

Bogdan Groza, Ioan Silea, Dragos Pop, Victor-Valeriu Patriciu

May 2009 ICIMP '09: Proceedings of the 2009 Fourth International Conference on Internet Monitoring and Protection

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

A framework of three attributes for video surveillance systems is underlined: availability, accessibility and authenticity. Under this framework, a scenario in which surveillance cameras can be accessed by remote devices, such as mobile phones, PDAs, over IP is addressed. Some security drawbacks of an off-the-shelf product are depicted and a ...

Keywords: video surveillance, availability, accessibility, authenticity

19 Cryptographic Authentication on the Communication from an 8051 Based Development Board over UDP

Bogdan Groza, Pal-Stefan Murvay, Ioan Silea, Tiberiu Ionica

June 2008 ICIMP '08: Proceedings of the 2008 The Third International Conference on Internet Monitoring and Protection

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

Implementing cryptography on devices with low computational power is a necessity as they became involved in communications over public networks. Even more, these devices became ubiquitous and are used in a large area of applications, from home-office systems to industrial control systems. We deal with the design and implementation of ...

20 Using a cryptographic authentication protocol for the secure control of a robot over TCP/IP

Bogdan Groza, Toma-Leonida Dragomir

May 2008 AQTR '08: Proceedings of the 2008 IEEE International Conference on Automation, Quality and Testing, Robotics - Volume 01

Publisher: IEEE Computer Society

Bibliometrics:

Citation Count: 0

The paper deals with the implementation of an authentication protocol, based on cryptographic techniques, that is used in the communication necessary for the control of a mobile robot over a public network. The robot is

connected via an 802.11 wireless network to a local computer; however the control of the ...