Research in Security and Privacy in Brazil

Marinho Barcellos | Federal University of Rio Grande do Sul
Diego F. Aranha | University of Campinas

The main research groups in Brazil working on the topics of security and privacy are characterized by both geographical distribution and research areas. The objective is to highlight the main contributions from these groups to the international community and discuss aspects of the research environment and the challenges ahead.

Security and privacy are arguably among the most important research topics today. With an increasingly connected society, the Internet rewriting older business models, and software quickly changing the world, security issues start to affect human life to a much greater extent. It is plausible to assume that autonomous systems will eventually comprise the majority of transport infrastructure, and a network of distributed sensors will help manage entire cities. Blockchains will decentralize financial systems and keep immutable public records about the world surrounding us. The foreseeable future will be shaped by communication technologies, and the Internet of Things (IoT) will challenge current illusions of privacy to levels never seen before.

In this context, secure and privacy-aware systems will make a difference by saving lives, protecting the economy from external interference, and preserving human rights. Brazil, one of the major economies on the planet, already faces security and privacy challenges in many fields. As one of the biggest exporters of commodities, production is increasingly automated and remotely monitored. Citizens vote for the next president using computer systems, and governments, both at the federal and the municipal scale, attempt to improve their services by leveraging the Internet. A booming start-up scene and entrepreneurship culture promise to improve the service sector using technology. Modernization offers attackers many new attack vectors, including ransomware, banking malware, and massive data breaches.

The major examples of digitization in the nation come from the government. In Brazilian elections since 2000, virtually every vote is cast through voting machines in an attempt to improve security and eliminate the rampant fraud in paper-based elections after the transition to democracy in 1985. In 2018 alone, the Department of Federal Revenue of Brazil received 29 million income tax declarations containing private data through the Internet. A recent trend is unifying the multiple official documents into a single smart card storing a certificate issued by the national public key infrastructure.

Digital Object Identifier 10.1109/MSEC.2018.2874855
Date of publication: 21 January 2019

 1540-7993/18©2018IEEE

Designing more secure and private systems for the future is paramount, and it is impossible to imagine this task being accomplished without a significant investment from academia. In this article, we characterize the main research groups in Brazil working on the topics of security and privacy when applied to many different scenarios. Researchers are grouped both by their distribution across Brazil's vast territory and their interests when tackling relevant questions in the field. We later summarize the main contributions from Brazilian researchers to the scientific literature in security and privacy.

Our methodology for data collection was straightforward. We started by collecting all names of program committee members from the past 10 editions of the Brazilian Symposium on Information and Computational Systems Security (SBSeg). Since 2005, SBSeg is the main scientific venue for research in security and privacy in Brazil, having grown out of a satellite workshop in the Brazilian Symposium on Computer Networks. We proceeded with grouping the researchers by institution and state in an attempt to characterize the research groups. This captured not only formal affiliation to a certain research group, for example, by working in the same laboratory, but also frequent collaboration between researchers in different but nearby institutions.

The next step was looking for Google Scholar profiles of the 86 selected researchers (mostly faculty in Brazilian universities), of which we found 73, amounting to 84.8 percent. Google Scholar was chosen because it is not only popular but a very inclusive source of scientific production and impact metrics, usually indexing sources ignored by other systems. From analyzing the Google Scholar profiles, we found the most highly cited works in the areas of cryptography, network security, and systems security. Although it is possible that we left out some relevant results by using this methodology, we believe it accurately captures the essence of the security and privacy research performed in Brazil. We also notice that research on privacy is still limited in the country and mostly based on cryptographic mechanisms and applications (homomorphic encryption and differential privacy); hence, the topic is discussed in the context of the technical security areas.

Research Environment

In this section, we outline the basic characteristics of performing research in security and privacy in Brazil, starting from the structure of research funding and then moving on to how research groups are organized and distributed.

Funding Structure

Research universities in Brazil are mostly public with a few exceptions, such as private universities maintained by the Catholic Church. Graduate schools are funded through a combination of resources: scholarships and financial support coming from federal agencies linked to Brazilian ministries, such as the Coordination for the Improvement of Higher Education Personnel (CAPES) and the National Council for Scientific and Technological Development (CNPq). Local governments have increasingly followed the example of the São Paulo Research Foundation (FAPESP) and have initiated or improved the participation of state agencies. Applied research and technological innovation are also frequently sponsored by federal funds specific to sectors in the economy, such as the Funding Authority for Studies and Projects (FINEP) and the National Scientific and Technological Development Fund (FNDCT). To a lesser degree, research is sponsored through partnerships with industry or international agreements with funding agencies in Europe and the United States. The Serrapilheira Institute, a private, nonprofit institution created to promote science in Brazil, is one of the latest additions to this list of science funding institutions.

In the context of jointly funded research projects in security and privacy, two specific examples are remarkable in reach and scope. In 2012, Intel Labs started the Intel Strategic Research Alliance for Energy-Efficient Security for System-on-Chip devices in Brazil, with a focus on exploring the implications of power constraints on the design and implementation of security in embedded systems. Grants funded projects in software implementation of cryptographic algorithms, field-programmable gate array (FPGA)-based intrusion detection systems, physical unclonable functions, security-aware program instrumentation, and efficient public-key cryptography for embedded devices. After the projects were finished, the initiative continued in collaboration with FAPESP, with smaller grants for research in side-channel countermeasures, hardware implementation aspects of postquantum cryptography, and hardware security mechanisms.

A partnership between the National Science Foundation (NSF) and Brazilian National Research and Educational Network (RNP) is fostering collaboration among researchers based in Brazil and the United States through five joint projects in cybersecurity. The corresponding open call received a stunning number of proposals (57, involving more than 200 researchers in the United States and Brazil). Topics addressed by selected projects span network security (including the IoT), Internet measurements, and programmable data planes for software-defined networks.

Main Groups and Their Distribution

There are many research groups in security and privacy scattered throughout Brazil. Research in systems

security is popular in the states of the North (Amazonas), Northeast (Rio Grande do Norte), Southeast (São Paulo and Minas Gerais), and South regions of Brazil (Paraná), whereas cryptography is heavily concentrated in the Southeast. Network security has the largest community and remains a preferred topic in a few groups in the Northeast (Ceará and Pernambuco) and the lower half of the country (Distrito Federal, Rio de Janeiro, Santa Catarina, Paraná, and Rio Grande do Sul). Figure 1 gives a map of this geographical distribution, using a color-coding scheme to denote topics ranking higher in interest at each of the universities to which these research groups belong.

- *North*. Researchers from the Federal University of Amazonas are part of the Emerging Technologies and Systems Security laboratory, specializing in web, software, and systems security.
- *Northeast*. The region includes the Networking and Telecommunication Research Group at the Federal University of Pernambuco (UFPE), specializing in traffic inspection and identification and security issues in wireless sensor networks, and the Group of Computer Networks, Software Engineering, and Systems at the Federal University of Ceará, working on network-level intrusion detection systems. An emerging research group at the Federal University of Rio Grande do Norte organized the 2018 edition of the SBSeg and is composed of researchers working in forensics, biometrics, and information security.
- *Central-West*. In the heart of the country, the Federal District has research groups at the University of Brasília working in computer networks with a focus on network security, in both the Computer Science Department and the Engineering School. Popular research topics are security issues in mobile ad hoc networks (MANETs), secure routing, and distributed systems. A research group in cryptography operated between 2011 and 2014 but was later dissolved due to the researchers' migration to other institutions.
- *Southeast*. The Laboratory of Security and Cryptography at the University of Campinas (UNICAMP) has a research group specializing in cryptographic engineering, security analysis of real-world systems, privacy-preserving computing, and malware detection and analysis. Researchers from the University of São Paulo were among the pioneers in cryptography, authoring the first books about the topic in Portuguese. Today, the Laboratory of Computer Networks and Architecture specializes in the design of cryptographic algorithms, protocols, and authentication schemes. The Federal University of Minas Gerais (UFMG) has researchers working on multiple areas: software security, key distribution in ad hoc networks, applied cryptography, electronic voting, differential privacy, and foundations of security. Rio de Janeiro has groups working on network security at the Federal University of Rio de Janeiro (UFRJ) and at the Fluminense Federal University, in the traditional topics of intrusion detection, trust management, key distribution, access control, and denial of service attacks. The National Institute of Metrology, Quality, and Technology also has a research group on smart metering and smart grid security.
- *South*. This region has the largest groups working on network and systems security. The state of Paraná has multiple research groups at the Federal University of Paraná and at the Pontifical Catholic University of Paraná in the topics of distributed systems, network and computer security, security issues in

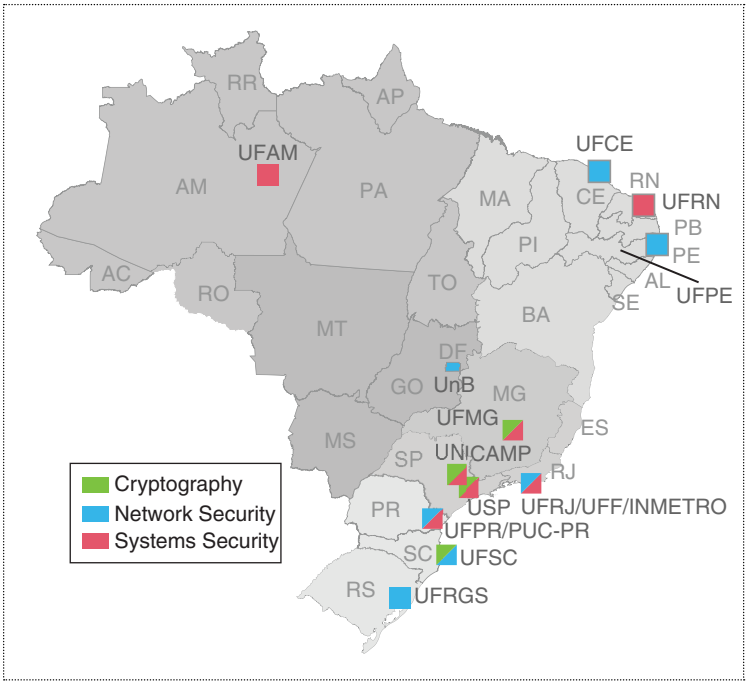

Figure 1. The distribution of the main research groups in security and privacy across Brazil. States without marked institutions do not appear to have formal groups participating closely in the local security and privacy research community, according to our data collection, and their names are not spelled out. The colors green, red, and blue denote interest in, respectively, cryptography, systems security, and network security. Multiple colors are used to represent research groups where multiple interests overlap. AM: Amazonas; CE: Ceará; DF: Distrito Federal; MG: Minas Gerais; PE: Pernambuco; PR: Paraná; RJ: Rio de Janeiro; RN: Rio Grande do Norte; RS: Rio Grande do Sul; SC: Santa Catarina; SP: São Paulo; PUC-PR: Pontifical Catholic University of Paraná; UFAM: Federal University of Amazonas; UFF: Fluminense Federal University; UFMG: Federal University of Minas Gerais; UFPE: Federal University of Pernambuco; UFPR: Federal University of Paraná; UFRGS: Federal University of Rio Grande do Sul; UFRJ: Federal University of Rio de Janeiro; UFRN: Federal University of Rio Grande do Norte; UFSC: Federal University of Santa Catarina; UNICAMP: University of Campinas; INMETRO: National Institute of Metrology, Quality and Technology; USP: University of São Paulo; UFCE: Federal University of Ceará; UnB: University of Brasília.

MANETs, virtualization, and malware analysis. Notable examples are the Network, Distributed Systems, and Security Lab; the laboratory on Wireless and Advanced Networks; and the Security and Privacy Laboratory. The state of Santa Catarina has multiple research groups at the Federal University of Santa Catarina (UFSC) and nearby institutions, working on operational security and public-key infrastructures (PKIs), intrusion detection and tolerance, grid and cloud computing, distributed systems, and identity management. The Computer Security Laboratory at UFSC has notably contributed to the implementation of the Brazilian-government-based PKI. Farther to the south, the Federal University of Rio Grande do Sul (UFRGS) has a research group on cybersecurity, reflecting its record of contributions to network security. The research topics investigated include network resilience, anomaly detection, botnets, security of the IoT for healthcare systems, security of software-defined networks, and in-the-wild studies of Internet security problems, such as spoofing.

Topics and Limitations

Scientific research is a challenging endeavor everywhere. Such research in Brazil is considered especially challenging due to the large cultural gap between the private sector and universities, even in applied research. With most funding depending on governments and their political whims, availability is very limited for certain types of projects and directs research toward topics that can be tackled under the restricted resources.

A simple example of this effect can be seen in cryptologic research, where Brazilian researchers rarely work in applied cryptanalysis due to insufficient access to supercomputing infrastructure. As a consequence, cryptologic research in Brazil is much more directed toward constructive and comparably inexpensive projects in cryptographic engineering and mathematical cryptography, although in some cases there are results in mathematical cryptanalysis of algorithms and protocols.

The same effect can be observed in network security, where researchers frequently complain about lack of access to modern datasets for traffic analysis and turn to software modeling and simulations as an alternative or rely on foreign sources, such as the Center for Applied Internet Data Analysis.[42] Ideally, this gap should be reduced in collaboration with security companies in the private sector, which ultimately face the daily threats of Internet-wide attacks and exploitation. Along the same lines, research on systems security is overwhelmingly directed to software mechanisms and protection, and hardware designs very rarely go beyond FPGA prototyping.

As a result, research is concentrated on technical security, with large areas not receiving enough attention. Some examples of these research topics involving human factors are usable security and economics of security. There is low general interest in privacy-enhancing technologies, which we speculate to be the result of cultural and historical factors. As eager and massive adopters of privacy-invasive social networks, Brazilians do not value privacy as much as other populations, and a strict reading of Article 5 in the Constitution limits anonymity: "the expression of thought is free, and anonymity is forbidden." The trend may be changing, with research groups recently working on differential privacy and privacy-preserving computing as applications of formal methods and homomorphic encryption mechanisms.

Main Contributions from the Brazilian Community

We detail the main contributions from researchers working in Brazil in three areas: cryptography, systems security, and network security. We selected the 20 most influential papers (the highest number of citations in Google Scholar) and then grouped them by similarity. A few exceptions were made for recent works that do not yet have a significant number of citations but that received awards or widespread coverage in the news.

Cryptography

Most of the contributions by Brazilian researchers in cryptography are concentrated in efficient algorithms and implementations of elliptic curve cryptography. The pioneering works by López and Dahab[1] at UNICAMP and by López in collaboration with Brown, Hankerson, and Menezes,[2,3] were among the first to propose efficient algorithms for implementing binary and prime curves standardized by the National Institute of Standards and Technology, demonstrating that binary curves could be a competitive choice for public-key cryptography. Following several papers through the years that introduced refinements and speedups for generic and Koblitz binary curves, the lambda coordinate system for representing points over these curves recently set the speed record for elliptic curves[4] and was recognized as the best paper at one of the area's most prestigious conferences (the 2013 Workshop on Cryptographic Hardware and Embedded Systems).

Brazilian researchers were also pioneers in the field of pairing-based cryptography. Barreto et al. essentially made pairing computation over elliptic curves practical by speeding up the performance-critical portions of the algorithm.[5] This was a very important contribution to the emerging field of pairing-based cryptography,

because pairing computation is a bottleneck on those cryptosystems. Barreto would spend most of the next decade proposing efficient pairing-based protocols,[6] compressed pairing computation, and efficient choices of parameters for instantiating pairings, such as the pairing-friendly Barreto–Naehrig family of elliptic curves.[7] The effort in improving the efficiency of pairings culminated in a very efficient implementation by Aranha et al.,[8] later made available with the RELIC[43] cryptographic library developed at UNICAMP.

The Brazilian research community has also worked in other aspects of cryptography. Researchers at the University of São Paulo led by Simplício, Jr., designed the Lyra2 algorithm,[9] selected as a finalist in the Password Hashing Competition, from which several features were adopted by the winner, Argon2. These algorithms are remarkably interesting, in the sense that both the latency and memory required per hashed password can be calibrated to penalize an offline attacker running on massively parallel platforms. In another research trend, the upcoming threat of quantum computers against conventional public-key cryptography motivates the field of postquantum (or quantum-safe) cryptography, a designation for cryptosystems based on underlying problems not known to be efficiently solved by quantum computers. One of the main contenders for encryption and key exchange protocols is code-based cryptography using moderate-density parity codes,[10] formally submitted as the BIKE[44] candidate to the NIST postquantum cryptography standardization project.

Other relevant contributions worth mentioning are solutions to the problem of key management in wireless sensor networks. Research efforts led by the UFMG produced many original and relevant contributions to this problem. SecLEACH was proposed by Oliveira et al. to adapt random key predistribution schemes from the usual flat networks to hierarchical cluster-based networks.[11] Later, Oliveira et al. also proposed TinyPBC[12] as a noninteractive key distribution protocol based on pairings, where nodes preloaded with private keys can compute a shared key without exchanging any messages. The protocol description was followed by an efficient implementation of pairing computation in sensor nodes to reduce the energy and execution time requirements. A good survey authored by Brazilian researchers on this topic can be found in the literature.[13]

Systems Security

Because this area significantly overlaps with network security and even cryptography (many cryptographers argue that cryptography is actually a systems problem), we employ here a loose definition of systems security by restricting it to system-level protection and excluding networking. Under this definition, Brazilian research groups have contributed to the foundations of computer security, electronic voting, and malware detection and analysis.

Controlling how much information leaks from communication channels is a fundamental problem in computer security. With this knowledge, a designer is better equipped to protect more vulnerable portions of the attack surface of a system. Alvim et al. have explored this problem in the context of quantitative information flow by introducing a generalization of previous models, such that an adversary can benefit from guessing parts or properties about a secret leak,[14] and by relating the information-theoretic models to the definition of differential privacy.[15] A later work on the same topic received the Best Scientific Cybersecurity Paper award from the National Security Agency in 2014.

Another rich set of contributions is available in the field of electronic voting systems, where researchers in Brazil have worked on both their design and security analysis. Santin et al. proposed an Internet-based voting protocol for coercion-free elections,[16] and Araújo et al. detected and fixed vulnerabilities in the ThreeBallot voting system and proposed a more secure and verifiable version based on Farnel.[17] In the specific case of the paperless Direct Recording Electronic (or DRE) voting system used in Brazil, the Brazilian Computer Society report[18] pioneered the first security analysis of the system and pointed out design flags in terms of ballot secrecy and insufficient guarantees for integrity. These threats would be experimentally demonstrated 10 years after by Aranha et al. during restricted tests organized by the national electoral authority.[19] The debate about security and transparency of the Brazilian voting system is still ongoing, especially after the recent congressional mandate for paper ballots to be implemented in future elections and the following Supreme Court decision to suspend the law.

System-level intrusion detection and malware analysis are also topics of interest. Brazilian researchers have designed bioinspired systems for detecting intruders by borrowing ideas from immune systems[20] and employing stealthy virtual machines for host-based detection.[21] Afonso et al. proposed a system using machine learning to detect if Android applications are malicious before the user can install them.[22] In application-level security, there are contributions in lightweight techniques to secure programs against integer overflows[23] and approaches based on machine learning to detect XSS attacks.[24]

Network Security

Chronologically, one of the first security problems to be addressed by the Brazilian research community was intrusion detection, with relevant papers appearing in

the late 1990s.[25,26] Another facet was the investigation of intrusion tolerance mechanisms, with a seminal paper published by Fraga and Powell.[27] Intrusion and anomaly detection remained a focus of the Brazilian community for many years, with varying contexts, such as virtualized environments and MANETs.[28]

The most relevant contributions about security of MANETs came from the 2000s.[29,30] Researchers from the UFPE and the UFRJ evaluated and proposed novel security mechanisms for these networks, including trust and reputation mechanisms. These groups made other contributions to Internet security around the same time, proposing improvements to traffic analysis[31] and spoofing countermeasures for Internet Protocol packets.[32]

The Internet context was also dominant in the studies carried out by researchers at the UFRGS. First, the group investigated the security of popular peer-to-peer protocols and was the first to identify attacks against BitTorrent and propose countermeasures.[33] The same group, in collaboration with the University of Twente, analyzed the problem of denial of service being offered as a service in the Internet.[34] Other contributions include security mechanisms for emerging network technologies, such as looking at IoT security for healthcare systems[35] and how to protect software-defined networks with a set of carefully positioned controllers.[36]

Besides advancing the state of the art in some direction, several Brazilian groups made contributions by surveying a topic of network security. Some leveraged their leadership and recognition to organize the body of work, whereas some performed systematic studies, often proposing a taxonomy for the field. These are magazine papers providing a summarized, higher-level view of a topic or longer surveys exploring a subject in both breadth and depth. Not surprisingly, areas typically reflect the contributions mentioned earlier but not necessarily by the same group. The more prominent examples are intrusion detection and cloud security,[37,38,39] MANETs,[40,13] and traffic analysis.[41]

Challenges and Perspectives

In the last two decades, the Brazilian research community in security and privacy has made substantial progress toward establishing an international presence through collaborations and contributions to the academic literature. However, additional effort must be dedicated if Brazil intends to become a global research power in this field. In this section, we provide some suggestions on how researchers can make further progress on the path ahead.

First, students, university staff, and faculty should improve their communication skills in English. Many interesting scientific contributions end up being restricted to the local community, after not receiving enough attention from the international community due to the inability of authors to effectively communicate their results internationally. This is also crucial for establishing productive collaborations with research groups abroad. Mobility should be actively fostered by bringing in and sending out expert researchers (including graduate students) to universities within and outside Brazil. Modern collaboration tools (videoconferencing and collaborative document editing) can help with the remaining cultural and logistic barriers.

Collaboration with the international research community may increase visibility and opportunity for broadening research topics, as evidenced by 21 of the works we highlighted that have at least one foreign coauthor. This effect is much higher in the area of cryptography, in which 10 of the 13 selected works were performed in collaboration with institutions abroad. This may also explain the higher visibility of research in cryptography, which scored the five most cited papers found in our data collection. We found a surprisingly low amount of collaboration between institutions located in different states among the highlighted works, corresponding to only five papers (or around 12 percent), of which only two involve authors from multiple regions. This suggests that an emphasis on longer-distance collaborations may be beneficial to the community. The NSF/RNP initiative for research in cybersecurity is a pioneer in this regard, fostering collaborations with the international community and also within Brazil, because four of the five funded projects include institutions from multiple states.

The Brazilian community should also reevaluate the high-priority research topics and trends, especially regarding privacy and network security, to keep up with the evolution of technology and the rise of new threats. In particular, privacy is key in any modern society, but substantial research in related aspects is notably missing in Brazil. State-of-the-art work appearing at the most prestigious security conferences should be closely monitored and the events attended with a higher frequency, despite funding limitations. This recommendation is, of course, not restricted to academic conferences, because industry and grassroots hacking events are wonderful opportunities to meet people, widen the range of contacts, and get access to data. Researchers should pursue high-risk/high-reward approaches to research and attempt to submit their results to top conferences even if the chance of acceptance is very low.

Adapting cutting-edge results to a Brazilian context is ultimately important, because the local scene is as globally relevant as that in any other country. By increasing the focus on security problems observed

in the wild, through research problems relevant to end users and companies, results may become more immediately useful to local communities, facilitating communication and cooperation with industry partners. ■

References

1. J. López and R. Dahab, "Fast multiplication on elliptic curves over GF(2^m) without precomputation," in *Proc. 1st Int. Workshop Cryptographic Hardware and Embedded Systems (CHES 1999)*, pp. 316–327.
2. M. Brown, D. Hankerson, J. López, and A. Menezes, "Software implementation of the NIST elliptic curves over prime fields," in *Proc. 2001 Conf. Topics Cryptology: Cryptographer's Track at RSA (CT-RSA 2001)*, pp. 250–265.
3. D. Hankerson, J. López, and A. Menezes, "Software implementation of elliptic curve cryptography over binary fields," in *Proc. 2nd Int. Workshop in Cryptographic Hardware and Embedded Systems (CHES 2000)*, pp. 1–24.
4. T. Oliveira, J. López, D. F. Aranha, and F. Rodríguez-Henríquez, "Two is the fastest prime: Lambda coordinates for binary elliptic curves," *J. Cryptographic Eng.*, vol. 4, no. 1, pp. 3–17, 2014.
5. P. S. L. M. Barreto, H. Yong Kim, B. Lynn, and M. Scott, "Efficient algorithms for pairing-based cryptosystems," in *Proc. 22nd Annu. Int. Cryptology Conf. (CRYPTO 2002)*, pp. 354–368.
6. P. S. L. M. Barreto, B. Libert, N. McCullagh, and J. Quisquater, "Efficient and provably-secure identity-based signatures and signcryption from bilinear maps," in *Proc. 11th Int. Conf. Theory and Application of Cryptology and Information Security*, 2005, pp. 515–532.
7. P. S. L. M. Barreto and M. Naehrig. "Pairing-friendly elliptic curves of prime order," in *Proc. 12th Int. Workshop Selected Areas in Cryptography (SAC 2005)*, pp. 319–331.
8. D. F. Aranha, K. Karabina, P. Longa, C. H. Gebotys, and J. López, "Faster explicit formulas for computing pairings over ordinary curves," in *Proc. 30th Annu. Int. Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT 2011)*, pp. 48–68.
9. E. R. Andrade, M. A. Simplício, Jr., P. S. L. M. Barreto, and P. C. F. dos Santos, "Lyra2: Efficient password hashing with high security against time-memory trade-offs," *IEEE Trans. Comput.*, vol. 65, no. 10, pp. 3096–3108, 2016.
10. R. Misoczki, J. Tillich, N. Sendrier, and P. S. L. M. Barreto, "MDPC-McEliece: New McEliece variants from moderate density parity-check codes," in *Proc. IEEE Int. Symp. Information Theory (ISIT 2013)*, pp. 2069–2073.
11. L. B. Oliveira, A. C. Ferreira, M. A. Vilaça, H. C. Wong, M. W. Bern, R. Dahab, and A. A. F. Loureiro, "SecLEACH—On the security of clustered sensor networks," *Signal Process.*, vol. 87, no. 12, pp. 2882–2895, 2007.
12. L. B. Oliveira, D. F. Aranha, C. P. L. Gouvêa, M. Scott, D. F. Câmara, J. López, and R. Dahab, "TinyPBC: Pairings for authenticated identity-based non-interactive key distribution in sensor networks," *Comput. Commun.*, vol. 34, no. 3, pp. 485–493, 2011.
13. M. A. Simplício, Jr., P. S. L. M. Barreto, C. B. Margi, and T. C. M. B. Carvalho, "A survey on key management mechanisms for distributed wireless sensor networks," *Comput. Netw.*, vol. 54, no. 15, pp. 2591–2612, 2010.
14. M. S. Alvim, K. Chatzikokolakis, C. Palamidessi, and G. Smith, "Measuring information leakage using generalized gain functions," in *Proc. 25th IEEE Computer Security Foundations Symposium (CSF 2012)*, pp. 265–279.
15. M. S. Alvim, M. E. Andrés, K. Chatzikokolakis, P. Degano, and C. Palamidessi, "Differential privacy: On the trade-off between utility and information leakage," in *Proc. 8th Int. Workshop Formal Aspects in Security and Trust (FAST 2011)*, pp. 39–54.
16. A. O. Santin, R. G. Costa, and C. Maziero, "A three-ballot-based secure electronic voting system," *IEEE Security Privacy*, vol. 6, no. 3, pp. 14–21, 2008.
17. R. Araújo, R. F. Custódio, and J. van de Graaf, *Towards Trustworthy Elections: New Directions in Electronic Voting*. New York: Springer-Verlag, 2010, pp. 274–288.
18. J. van de Graaf and J. R. F. Custódio. (2002). Electoral technology and the voting machine—Report of the Brazilian Computer Society (in Portuguese) [Online]. Available: http://www.sbc.org.br/index.php?option=com_jdownloads&Itemid=195&task=view.download&catid=77&cid=107
19. D. F. Aranha, M. M. Karam, A. Miranda, and F. Scarel, "Software vulnerabilities in the Brazilian voting machine," in *Design, Development, and Use of Secure Electronic Voting Systems*. Hershey, PA; IGI Global, 2014, pp. 149–175.
20. F. S. Paula, L. N. de Castro, and P. L. de Geus, "An intrusion detection system using ideas from the immune system," in *Proc. IEEE Congress on Evolutionary Computation (CEC 2004)*, pp. 1059–1066.
21. M. Laureano, C. Maziero, and E. Jamhour, "Protecting host-based intrusion detectors through virtual machines," *Comput. Netw.*, vol. 51, no. 5, pp. 1275–1283, 2007.
22. V. M. Afonso, M. F. de Amorim, A. R. A. Grégio, G. B. Junquera, and P. L. de Geus, "Identifying Android malware using dynamically obtained features," *J. Comput. Virology Hacking Techniques*, vol. 11, no. 1, pp. 9–17, 2015.
23. R. E. Rodrigues, V. H. S. Campos, and F. M. Q. Pereira, "A fast and low-overhead technique to secure programs against integer overflows," in *Proc. IEEE/ACM Int. Symp. Code Generation and Optimization (CGO 2013)*, pp. 33: 1–33:11.
24. A. E. Nunan, E. Souto, E. M. dos Santos, and E. Feitosa, "Automatic classification of cross-site scripting in web pages using document-based and URL-based features," in *Proc. IEEE Symp. Computers and Communication (ISCC 2012)*, pp. 702–707.

25. J. M. Bonifácio, A. M. Cansian, A. C. P. L. F. de Carvalho, and E. S. Moreira, "Neural networks applied in intrusion detection systems," in *Proc. IEEE Int. Joint Conf. Neural Networks (IJCNN 1998)*, pp. 205–210.
26. J. D. de Queiroz, L. F. R. da Costa Carmo, and L. Pirmez, "Micael: An autonomous mobile agent system to protect new generation networked applications," in *Proc. Recent Advances in Intrusion Detection (RAID 1999)*.
27. J. S. Fraga and D. Powell, "A fault-and intrusion-tolerant file system," in *Proc. of the 3rd Int. Conf. Computer Security*, 1985, 203–218.
28. R. S. Puttini, J. Percher, L. Mé, O. Camp, R. T. de Sousa Júnior, C. J. B. Abbas, and L. J. García-Villalba, "A modular architecture for distributed IDS in MANET," in *Proc. Int. Conf. Computational Science and Its Applications (ICCSA 2003)*, pp. 91–113.
29. G. Guimarães, E. Souto, D. F. H. Sadok, and J. Kelner, "Evaluation of security mechanisms in wireless sensor networks," in *Proc. 2005 Systems Communications*, pp. 428–433.
30. P. B. Velloso, R. P. Laufer, D. de Oliveira Cunha, O. C. M. B. Duarte, and G. Pujolle, "Trust management in mobile ad hoc networks using a scalable maturity-based model," *IEEE Trans. Netw. Service Manag.*, vol. 7, no. 3, pp. 172–185, 2010.
31. A. C. Callado, J. Kelner, D. Sadok, C. A. Kamienski, and S. F. L. Fernandes, "Better network traffic identification through the independent combination of techniques," *J. Netw. Comput. Appl.*, vol. 33, no. 4, pp. 433–446, 2010.
32. R. P. Laufer, P. B. Velloso, D. O. Cunha, I. M. Moraes, M. D. D. Bicudo, M. D. D. Moreira, and O. C. M. B. Duarte, "Towards stateless single-packet IP traceback," in *Proc. 32nd Annu. Conf. Local Computer Networks (LCN 2007)*, pp. 548–555.
33. M. A. Konrath, M. P. Barcellos, and R. B. Mansilha, "Attacking a swarm with a band of liars: Evaluating the impact of attacks on BitTorrent," in *Proc. 7th IEEE Int. Conf. Peer-to-Peer Computing (P2P 2007)*, pp. 37–44.
34. J. J. Santanna, R. van Rijswijk-Deij, R. Hofstede, A. Sperotto, M. Wierbosch, L. Z. Granville, and A. Pras, "Booters—An analysis of DDoS-as-a-service attacks," in *Proc. IFIP/IEEE Inter. Symp. Integrated Network Management (IM 2015)*, pp. 243–251.
35. L. M. R. Tarouco, L. M. Bertholdo, L. Z. Granville, L. M. R. Arbiza, F. J. Carbone, M. A. Marotta, and J. J. C. de Santanna, "Internet of Things in healthcare: Interoperatibility and security issues," in *Proc. IEEE Int. Conf. Communications (ICC 2012)*, pp. 6121–6125.
36. L. F. Müller, R. R. Oliveira, M. C. Luizelli, L. P. Gaspary, and M. P. Barcellos, "Survivor: An enhanced controller placement strategy for improving SDN survivability," in *Proc. IEEE Global Communications Conf. (GLOBECOM 2014)*, pp. 1909–1915.
37. K. Vieira, A. Schulter, C. B. Westphall, and C. M. Westphall, "Intrusion detection for grid and cloud computing," *IT Prof.*, vol. 12, no. 4, pp. 38–43, 2010.
38. N. M. Gonzalez, C. Miers, F. F. Redígolo, M. A. Simplício, Jr., T. C. M. B. Carvalho, M. Näslund, and M. Pourzandi, "A quantitative analysis of current security concerns and solutions for cloud computing," *J. Cloud Computing*, vol. 1, July 2012. doi: 10.1186/2192-113X-1-11.
39. A. Patel, M. Taghavi, K. Bakhtiyari, and J. Celestino Júnior, "An intrusion detection and prevention system in cloud computing: A systematic review," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 25–41, 2013.
40. M. N. Lima, A. L. dos Santos, and G. Pujolle, "A survey of survivability in mobile ad hoc networks," *Commun. Surveys Tuts.*, vol. 11, no. 1, pp. 66–77, 2009.
41. A. C. Callado, C. A. Kamienski, G. Szabo, B. P. Gero, J. Kelner, S. F. L. Fernandes, and D. F. H. Sadok, "A Survey on Internet traffic identification," *Commun. Surveys Tuts.*, vol. 11, no. 3, pp. 37–52, 2009.
42. Center for Applied Internet Data Analysis. (2018). Traffic analysis research. [Online]. Available: https://www.caida.org/research/traffic-analysis/
43. D. F. Aranha and C. P. L. Gouvêa. RELIC is an efficient library for cryptography. [Online]. Available: https://github.com/relic-toolkit/relic
44. The BIKE team. BIKE—Bit flipping key encapsulation. [Online]. Available: http://bikesuite.org/

Marinho Barcellos is an associate professor at the Federal University of Rio Grande do Sul. He is a 1D level researcher with the National Council for Scientific and Technological Development and a senior member of the Association for Computing Machinery and the Brazilian Computer Society. His current research interests include Internet measurements, programmable data planes, and security aspects of those networks. He has authored many papers on computer networks and security. Contact him at marinho@inf.ufrgs.br.

Diego F. Aranha is an assistant professor at the University of Campinas. His research interests include cryptography and computer security, with a special interest in the efficient implementation of cryptographic algorithms and security analysis of real-world systems. He has twice received the Google Latin America Research Award for research on privacy, and he also received the *MIT Technology Review* Innovators Under 35 Brazil Award for his work in electronic voting. Contact him at dfaranha@ic.unicamp.br.