Cybersecurity and Privacy Issues in Brazil: Back, Now, and Then

Daniela Seabra Oliveira | University of Florida
Jeremy Epstein and James Kurose | National Science Foundation
Anderson Rocha | University of Campinas (UNICAMP)

The goal of this special issue is to showcase cutting-edge research on security and privacy issues in Brazil, with a focus on topics that reflect Brazil's unique security and privacy challenges. Why Brazil? First, Brazil is the largest country in Latin America, with more than 200 million people. It is the fifth largest and the sixth most populous country in the world, with a rapidly developing economy (the world's eighth richest). Brazil is also a major player in cybersecurity. Further, Brazil's capabilities in cybersecurity have grown in the past several years, as reflected by a recent joint government- and academia-led pair of workshops involving the security communities of Brazil and the US (www.usbrazilsec.org) as well as a US–Brazil program funded by the US National Science Foundation (NSF) and the Brazilian Ministry of Science, Technology, Innovation and Communication (MCTIC).[1] Many peculiarities and challenges related to cybersecurity and privacy are unique to Brazil and so warrant special attention from the international cybersecurity community because of their potential to inform future global cybersecurity initiatives.

The Special Issue

This call for papers received 23 submissions, of which five were accepted after a careful peer-review process involving reviewers from academia, industry, and government agencies in the US, Brazil, and Europe. The accepted articles focus on diverse themes related to Brazil's cybersecurity and privacy issues, such as the general ecosystem of cybersecurity research in Brazil, e-voting and security vulnerabilities, banking malware, secure platforms for capture-the-flag (CTF) competitions, and intercontinental data processing cloud systems.

Digital Object Identifier 10.1109/MSEC.2018.2874824
Date of publication: 21 January 2019

The first article, "Research in Security and Privacy in Brazil," by Marinho Barcellos and Diego F. Aranha, presents a panorama of the kinds of research conducted in Brazil, characterizes the main research groups, and highlights the primary contributions these groups have made to the international community. The article also touches on aspects of the research environment and the challenges ahead.

From the research panorama, we delve into the details of e-voting in Brazil. In the article "The Good, the Bad, and the Ugly: Two Decades of E-Voting in Brazil," Diego F. Aranha and Jeroen van de Graaf present a critical discussion of e-voting in the country showing that, despite Brazil having pioneered nationwide e-voting in the 1990s, the voting system still faces challenges regarding auditability and verifiability.

Veering away from e-voting systems to the plague of malware, the article "The Need for Speed: An Analysis of Brazilian Malware Classifiers," by Fabrício Ceschin, Felipe Pinagé, Marcos Castilho, David Menotti, Luiz S. Oliveira, and André Grégio, argues that using conventional learning systems alone—without taking into account changes in concept—decreases the performance of classification of malware targeting Brazil, thus motivating model updates immediately after concept drift takes place.

Next, "NIZKCTF: A Noninteractive Zero-Knowledge Capture-the-Flag Platform," by Paulo Matias, Pedro Barbosa, Thiago N.C. Cardoso, Diego M. Campos, and Diego F. Aranha, discusses the importance of CTF competitions for the Brazilian cybersecurity community as educational and professional tools and introduces the first open-audit CTF platform based on noninteractive zero-knowledge proofs aimed at mitigating security problems in existing CTF platforms.

Finally, moving to cloud-based cybersecurity challenges, the article "A Europe–Brazil Context for Secure Data Analytics in the Cloud," by Paulo Silva, Tania Basso, Nuno Antunes, Regina Moraes, Marco Vieira, Paulo Simões, and Edmundo Monteiro, presents an interesting examination of intercontinental data processing cloud systems and their inherent security and privacy challenges, particularly due to legislative differences. Considering the context of Brazil and the EU, the authors propose solutions for these challenges by means of elastic authentication, authorization, and accounting; efficient privacy and anonymization techniques in multiple phases; and security assessment for trustworthiness estimation.

Looking Forward

If you are a researcher in a science or engineering discipline, chances are that others with interests most closely aligned to your own are not in the office next door, not in your university, and not even in your country. Scientific research is international, with the best and brightest minds in research areas being explored around the world. In fact, researchers are increasingly engaged in international collaborations. According to the Science and Engineering Indicators 2016 report,[2] the percentage of publications with authors from multiple countries rose from 13.2 to 19.2 percent between 2000 and 2013. Based on our own experience at NSF's Directorate for Computer and Information Science & Engineering (Kurose and Epstein) and as researchers with international collaborators (all authors), there are a few common ingredients associated with developing and launching a successful collaborative international research program.

- *People and people connections*. The researchers themselves are at the heart of any collaboration, and, in the end, they want to work with the best minds in the world.[3] In some cases, completely new collaborations may arise from a collaborative research funding opportunity; in other cases, they build on informal or formal past collaborations. The foundations for such past collaborations may have been laid by programs supporting research visits by students and faculty in either direction. For example, Kurose and Oliveira have, for separate projects, worked with Brazilian students and faculty who have traveled to the US with funding from the Brazilian National Council for Scientific and Technological Development and also from the NSF. Rocha has been working with students from abroad who receive funds from the EU, DARPA, the Singapore government, and France's Agence Nationale de La Recherche.
- *Topic area*. For a collaborative research program focused on a specific area (as in the US–Brazil Collaboration on Cybersecurity Research[1]), the topic must be important to both countries' research communities and aligned with national (funding agency) priorities. There must also be a critical mass of world-class researchers in that topic area—researchers who are excited about international collaboration and what that entails (for example, traveling and researcher exchanges). And each side must bring unique and complementary perspectives, strengths, and opportunities to the table. Will the collaboration advance important research not otherwise possible? Will it accelerate the pace of research development? Will it provide opportunities for students or early career researchers who have not yet had the chance to participate in international collaborations? Will it provide access to unique resources?
- *Agency-to-agency leadership and collaboration*. Just as there must be excitement among researchers, so, too, must there be excitement within the recognized funding

agencies. A "champion" in each agency provides vision and does the hard work needed to make a collaborative research opportunity happen. In the case of the US–Brazil Collaboration on Cybersecurity Research,[1] numerous agency leaders at the Center for Research and Development in Digital Technologies for Information and Communication, the National Research and Educational Network, and the MCTIC in Brazil and the NSF in the US have been critical in providing the vision, hard work, and leadership to make the collaboration a reality. This funding opportunity would not have happened without their tremendous efforts.

- *Research community leadership*. Leaders within the research communities play a crucial role in organizing and spurring international research opportunities. They have a vision for the potential and value proposition of international research collaboration, and they can articulate that vision. They often organize workshops that bring together the research community to identify topic areas for possible collaboration and build research-to-researcher connections.

We hope this issue provides readers with an informative, albeit small, sample of research on cybersecurity and privacy issues pertaining to Brazil. And we sincerely hope this can foster future multicountry initiatives and collaboration to solve pressing global cybersecurity and privacy challenges. ■

Acknowledgments

Any opinions, findings, and conclusions or recommendations expressed in this material by Kurose and Epstein are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

1. J. Kurose and L. Z. Granville. (2016, Oct.). Dear colleague letter: Enabling US–Brazil collaboration on cybersecurity research. National Science Foundation. Arlington, VA. NSF 17-024. [Online]. Available: https://nsf.gov/pubs/2017/nsf17024/nsf17024.jsp?org=NSF
2. National Science Board. (2016). Science and engineering indicators 2016. [Online]. Available: https://www.nsf.gov/statistics/2016/nsb20161/#/
3. Royal Society. (2011, Mar.). Final report—Knowledge, networks and nations. [Online]. Available: https://royalsociety.org/topics-policy/projects/knowledge-networks-nations/report.

Daniela Seabra Oliveira is an associate professor in the Department of Electrical and Computer Engineering at the University of Florida. Her research interests include interdisciplinary computer security, where she employs successful ideas from other fields to make computer systems more secure, and usable and systems security. Oliveira received a Ph.D. in computer science from the University of California at Davis. She was honored with a National Science Foundation CAREER Award in 2012; the 2014 Presidential Early Career Award for Scientists and Engineers (presented by President Obama); and the 2017 Google Security, Privacy, and Anti-Abuse Award. Her research has been sponsored by the National Science Foundation, DARPA, the MIT Lincoln Laboratory, the National Institutes of Health, and Google. Contact her at daniela@ece.ufl.edu.

Jeremy Epstein is the deputy division director for the National Science Foundation's Division of Computer and Network Systems in the Directorate for Computer and Information Science and Engineering. His research interests include cybersecurity with a particular focus on election systems. Epstein received an M.S. in computer science from Purdue University, and is ABD in information technology from George Mason University. He is an associate editor-in-chief of *IEEE Security & Privacy*, a senior member of ACM, and a Senior Member of the IEEE. Contact him at jepstein@nsf.gov.

James Kurose is a distinguished university professor in the College of Information and Computer Sciences at the University of Massachusetts Amherst and assistant director at the National Science Foundation, where he leads the Directorate of Computer and Information Science and Engineering. He received a Ph.D. in computer science from Columbia University. He is a fellow of ACM and a Fellow of the IEEE. Contact him at jkurose@nsf.gov.

Anderson Rocha is an associate professor and associate dean in the Institute of Computing, University of Campinas (UNICAMP), Brazil. His main research interests include digital forensics, reasoning for complex data, and machine intelligence. He is an associate editor of *IEEE Transactions on Information Forensics and Security*, *Journal of Visual Communication and Image Representation*, *Journal on Image and Video Processing*, and *IEEE Security & Privacy* magazine. He is an elected affiliate member of the Brazilian Academy of Sciences and the Brazilian Academy of Forensic Sciences as well as a Microsoft Research and a Google Research Faculty Fellow and, in 2016, he was awarded the Tan Chin Tuan Fellowship. He is a Senior Member of the IEEE. Contact him at anderson.rocha@ic.unicamp.br.