

US Brazil Research Collaborations – Opportunities and Challenges

This document describes the discussions of four working groups during two afternoons at the US Brazil Workshop on Cyber Security and Privacy, held at Orlando, FL on April 7 and 8 2016.

Group 1

Participants: David Ott (Intel), Daniel Batista (University of Sao Paulo), Matt Bishop (UC Davis), Marco Carvalho (Florida Institute of Technology), Scott Condie (Brigham Young University), David Dittrich (University of Washington), Jorge H.C. Fernandes (University of Brasilia), Joao Gondim (University of Brasilia), Andre Gregio (CTIC/UNICAMP), Yao Liu (University of Southern Florida), Altair O. Santin (Catholic University of Parana), Jeroen van de Graaf (Federal University of Minas Gerais)

Leader/Scribe: David Ott (Intel)

1. US-Brazil Collaboration Benefits/Opportunities

Session participants were asked to discuss the benefits of international collaboration as a way of focusing program opportunities and potential features. Their ideas were as follows:

- **Better science by studying two different technology ecosystems.** Security researchers can clearly benefit from the way projects will consider two different technology ecosystems (i.e., that of the US and Brazil). The researchers felt that this aspect of the program would broaden their understanding of security challenges and solutions. For example, by considering two different ecosystems, it becomes clearer what security challenges are inherent to technology ecosystems in general, and what challenges are best understood as ecosystem-specific. Not only would they learn more about another ecosystem, it would better help them to understand their own ecosystem with greater clarity. Participants found it easy to identify technical domains with compelling mixes of commonalities and differences -- banking applications, security exchanges, voting, technology user behavior, organizational behavior, privacy laws and cultural norms, social groups (e.g., elderly), physical environments (which influence SLA requirements), network infrastructure (which influences attack types), among others.
- **More robust solutions.** Not only do separate technology ecosystems help in understanding security challenges, they are useful in developing and testing solutions. Solutions striving for universality could be tested in both ecosystems to better understand effectiveness.
- **Special opportunities and resources.** “Research pitch” presentations mention many university-specific and country-specific resources that could benefit researchers who typically do not have access. For example, University of Brasilia’s CEGSIC (2012-2014) data and results are highly unique, as are UC San Diego’s CAIDA internet measurement data.
- **Expanded domain of impact.** Researchers were generally excited at the prospect of their work having greater impact and visibility within two countries (and continents) rather than one. This

includes dissemination of results within academic circles, the sharing of data collection efforts, and the impact of solutions that promise applicability in both countries.

- **Expanded research capabilities.** The US-Brazil international collaboration promises stronger research teams than what funding can buy in each country independently. US researchers, for example, appreciate the extended research capabilities that results from additional Brazilian researchers funded by the Brazilian funding sources. The converse is true of Brazilian researchers.
- **Benefits to researchers.** Researchers from each country value the opportunity to broaden their understanding of technology ecosystems by their exposure to another country. The perspective they gain will be invaluable in selecting future research problems, developing more universal approaches, understanding the ecosystem-specific aspects of their own countries, and generally discerning what is important and what is not in cyber security research
- **Benefits to students.** Graduate student researchers are tomorrow's professors, researchers, and technology leaders. As such, it is important to note that their learning experience will be enhanced by the international collaboration, providing them with international technology perspectives, exposure to students and PIs at another institution, and experience with a broader set of data collection, software, and research tools. This is especially true if the program supports exchanges where students have the opportunity to live and work in the other country for an extended period of time (e.g., several weeks or months).
- **Building a country-neutral research community.** The trading of information and solutions across borders builds an international cyber security research community that is stronger than any individual country. For example, the exchange of vulnerability information builds a stronger picture of vulnerabilities than a single country can construct.

2. Project/Program Structure

- **Researcher's interactions.** Researchers imagine US-Brazil interactions to be as follows:
 - *Weekly or bi-weekly teleconference project meetings.* Such meetings include student researchers who often lead discussion of work in progress.
 - *Face-to-face project meeting in Brazil once per year.* Once each year, all researchers (PIs and students) meet face-to-face in Brazil for a week to discuss research.
 - *Face-to-face project meeting in the US once a year.* Once each year, all researchers (PIs and students) meet face-to-face in the US for a week to discuss research.
- **US-Brazil program-level events**

- *Kickoff workshop event.* Participants felt this would be important, especially for the students newly involved in the research effort.
 - *Annual workshop event.* Meeting once a year for a workshop event would provide an opportunity to present results and exchange information between research projects. Workshop locations could alternate between the US and Brazil.
- **Reporting**
 - Brazil PIs could provide a standard report to CNPq at the completion of the project.
 - US PIs could provide a standard yearly report to NSF once each year.

3. Research expense profiles

The researchers discussed major expense types for their research, and differences between the US and Brazilian academic funding models. Below is a summary of high-level budget items to be considered.

Brazil	US
<ul style="list-style-type: none"> • Equipment • People <ul style="list-style-type: none"> • 2 PhD student scholarships • 1 Post-doc (if possible) • Travel funding (for PI and students) <ul style="list-style-type: none"> • 2 international conferences • 1 face-to-face meeting in US • Extended US stay (if possible) 	<ul style="list-style-type: none"> • Equipment • People <ul style="list-style-type: none"> • 1-2 non-resident PhD student tuition/stipend • 1 Post-doc (if possible) • Summer PI salary • Research staff expenses (as applicable) • Travel funding (for PI and students) <ul style="list-style-type: none"> • 2 international conferences • 1 face-to-face meeting in Brazil • Extended Brazil stay (if possible) <p><i>Notes:</i></p> <ul style="list-style-type: none"> • US professors are on a 9-month salary. • Some US PIs rely entirely on research funding for their salary. • US universities charge significant overhead.

About travel funding, all participants felt that it would be valuable for PIs and/or students to stay in their partner country for an extended stay (e.g., several weeks or a month). Students, in particular, would benefit from the arrangement.

4. Additional Issues

- **Number of PIs.** A minimal research team would be comprised of one Brazilian PI and one US PI. But participants wondered how many PIs program sponsors would allow for a single proposal. Similarly, how many subprojects or research threads might be supported for a given proposal? Such questions have implications for the scoping of research and the number of students requested.
- **Start Timing / Calendar Synchrony.** Participants agreed that it is important to start US and Brazil research project funding at the same time (i.e., that research teams are synchronized for the 2-year research period). Participants observe that academic calendars in the two countries look roughly as follows:
 - Brazil: Semester 1 is March through June. Semester 2 is August through November. Vacation periods are January-February and July.
 - US: Semester 1 is late August through early December. Semester 2 is January through mid May. Vacation periods are mid December through early January and select summer periods.

Participants observe that the two semesters are actually quite similar in timing, but that semesters 1 and 2 are swapped between the two countries. Target start periods should be August and late February or early March.

- **Intellectual property.** In general, professors are bound by their university policies on IP. Participants note, however, that open IP is a desirable arrangement that promotes collaboration across organizations and avoids obstacles across borders
- **Data availability and archiving.** Participants felt strongly that the program should consider ways to make research data available during and after the period of funded research.

Group 2

Participants: Kimberly Claffy (CAIDA, University of San Diego), Micah Sherr (Georgetown University), Michele Mazurek (University of Maryland, College Park), Marinho Barcellos (Federal University of Rio Grande do Sul), Jeremy Epstein (DARPA), Brad Huffaker (CAIDA, University of San Diego), Kevin Butler (University of Florida), Anna Squicciarini (Pennsylvania State University), Ken Calvert (NSF), Edmundo de Souza e Silva (Federal University of Rio de Janeiro), Fabio Tagnin (Intel)

Leader/Scribe: Kimberly Claffy (CAIDA, University of San Diego)

1. US-Brazil Collaboration Benefits/Opportunities

A U.S. Brazil collaboration offers opportunities through increased diversity in human-related data samples; different cultural perspectives, and under-tapped raw talent. Both countries have vibrant open source communities, extensive mobile device penetration, and non-trivial IPv6 deployment. These factors could facilitate many comparative research students related to cybersecurity.

One researcher noted a cybersecurity-relevant difference: in Brazil, many people exclusively use their mobile device in lieu of landline access, and as a result, mobile devices often don't take security updates promptly because it counts against their data cap. The two countries also face similar policy issues with regard to the tension between ISPs and content providers (network neutrality), and facilities based competition.

The two countries also both have pockets of strong research interest in future Internet architecture research, especially information-centric networking, which provides a terrific opportunity for NSF to continue its substantial investment in this area as it gains international momentum.

Cost-sharing can leverage the collaboration to allow more coordinated investment in a single research area.

2. US-Brazil Collaboration Challenges

The group discussed several challenges to academic research collaborations between the United States and Brazil. Some challenges stem from the difficulty of aligning project funding and resources. In Brazil, most funding for students tends to flow directly to universities, while in the U.S. universities compete for student funding through peer-reviewed proposals.

More specifically, in Brazil, the traditional post-graduate programs receive some number of funded PhD student slots to assign to students. Different universities may have different approaches to allocating these slots. In some departments, student standardized test scores (CSE GRE) drive these allocations. Grants are for four year increments. Students can thus more easily change their projects as their interest changes, with no implications for their own funding since it does not usually link directly to a project. Project-specific funding tends to support equipment and travel.

The overhead differences are substantial: Brazilian universities charge no overhead to grants from some Brazilian government agencies, whereas U.S. universities charge 50% or more overhead to federal funding agencies. Any cost-matching requirements across the two countries will need to accommodate these differences in traditional flows of funding. The cost-of-living differences also pose some challenges in the context of each country supporting costs of hosting exchange students. A specific issue noted is that Brazil pays travel/expenses for Brazilians traveling to the U.S., but do not pay university fees (which may not pose a problem if the student is not taking classes in the U.S.).

Other administrative challenges include the differences in proposal format, metrics for review, reporting format and frequency. To the extent possible, the program should unify proposals and reporting formats so that researchers only have to submit them once. The program should also unify the metrics for evaluating proposals. The U.S. and Brazil agencies may want to consider also unifying any associated institutional ethical review process, although this is a more complex and evolving issue. Other challenges identified included the potential short grant duration (24 months?), and limits on the number of proposals per PI per year, while collaborations are still being explored.

Challenges related to information sharing and data management were also noted. It is already difficult for researchers to get relevant measurements and data sets from industry, and crossing national boundaries might present different challenges.

Group 3

Participants: Diego Aranha (UNICAMP), Fabian Monroe (University of North Carolina), Anderson Nascimento (University of Washington, Tacoma), Ricardo Custódio (Federal University of Santa Catarina), Mário Alvim (Federal University of Minas Gerais), Jean Martina (Federal University of Santa Catarina), Marcos Simplício (University of Sao Paulo), Ann Cox (DHS), David Dittrich (University of Washington), Willian Robertson (Northeastern University), Stephanie Okimoto (DHS)

Leader/Scribe: Diego Aranha (UNICAMP)

1. US-Brazil Collaboration Benefits/Opportunities

Critical infrastructure and government communication have been repeatedly exposed as vulnerable in the past decade, representing a formidable obstacle to human progress. Funding international collaborations in cybersecurity is fundamental to solve these important problems, many of interdisciplinary nature and combining technological aspects with human factors. Elegant solutions will most likely require the involvement of researchers with different backgrounds and points of view, and a U.S./Brazil research initiative is critical in that direction. Furthermore, the expected applied nature of the developed projects may produce innovative solutions not restricted to an academic setting, but present new development and business opportunities. Researchers from this breakout group discussed challenges in several stages of a project execution: namely: design and formulation, submission and operation.

This initiative has remarkable potential and presents many opportunities for the two communities. First of all, involving researchers from different countries will likely develop original solutions to problems prevalent in the two countries. Exposure to different problems will certainly pose unique opportunities for joint research and increase potential impact, especially when the effect of different cultural aspects, organization of the governments and critical infrastructure is considered. A few examples of topics where the countries significantly differ are electronic voting, banking and financial systems, identity management mechanisms, power grid security, defense sector, privacy awareness and perception of trust in technology.

The two countries also have very different policies for data protection and distribution, making diverse databases available for research purposes. Moreover, there is also clear potential for increased internationalization of Brazilian graduate programs, due to a higher influx of international students. It is standard practice in Brazilian graduate schools to send students abroad for a 1- or 2-year exchange, and this would work better if such exchanges happen under formal projects. The exchange of human resources between the two countries presents opportunities for improving quality of cybersecurity education and indirectly benefiting other countries in Latin America.

2. US-Brazil Collaboration – Administrative recommendations

Submitted projects should aim at bootstrapping international collaboration among researchers in cybersecurity. In order to fulfill this role, we considered that ideal projects should span a period 24 months, with a well-articulated milestone in the middle. Objectives should be aligned with this schedule, so yearly renewal is likely and review can be made based on actual evidences of progress.

Projects should aim for applied research in one of three tracks: security/privacy, cyber-physical systems and IoT, malware/cybercrime. Cryptography was not explicitly covered in the topics, but the conclusion is that applied cryptography will naturally support several of the projects. The funding in the proposals could match two reference projects. In the US side, projects should be calibrated to match the NSF small project. In the Brazilian side, we considered as reference a recently-implemented Intel/FAPESP project supporting 1 postdoc, 3 MSc students and 2 undergrads: around 150K BRL per year.

Note that this does not consider special equipment needs and PhD students were not taken into account due to the length of the project. Acquiring special equipment may impose huge taxes and import delays, so projects should be careful with equipment, perhaps keeping more equipment in the US side and more personnel in the Brazilian one, if that is the case. Funded items should mainly include scholarships, participation in PI meetings, traveling to conferences and extended stays when sending students abroad. We suggest having one PI meeting per year and planning for at least two 2-week visits per year for PIs and

students. Beware that funding will be executed by different systems, thus organizing the collaboration with a detailed schedule is critical and the submissions should accurately reflect that.

The submission/evaluation process should avoid restricting applications to submissions already approved by Institutional Review Boards (IRBs) and imposing too strict limits on the number of PIs and submissions. There was consensus that multiple submissions per PI should be allowed if they focus on different research tracks among the listed. We found reasonable to limit total number submissions to 2 per PI. Multiple PIs per submission should be allowed too, because researchers are reporting multiple interests and preference for many small projects over a few large ones, since the objective is to bootstrap collaborations.

The review process should be coordinated and have a reconciliation step to avoid strikingly different reviews from the two sides. The process should involve Brazilian researchers upfront, with virtual panel participation, following NSF practices due to higher experience. RNP/Brazil and SaTC may have useful guidelines and standard practices to contribute. Finally, some operations aspects are desired to allow healthy progress in the approved projects. The ideal frequency of reports would be at every 6 months, as 3-month milestones are too disruptive to research endeavors. Intellectual property issues should be resolved at the beginning, to prevent obstacles against international collaborations.

Group 4

Participants: Wagner Meira (Federal University of Minas Gerais), Daniel Figueiredo (Federal University of Rio de Janeiro), and Luiz Rust (INMETRO/Federal University of Rio de Janeiro)

Leader/Scribe: Wagner Meira (Federal University of Minas Gerais)

1. US-Brazil Collaboration Benefits/Opportunities

Opportunities For Both Countries:

The group envisages the following opportunities for both countries:

- Fostering cross-country teams: this is one of the key motivations for establishing collaborations. Cross-country teams would not only work together and exchange ideas and technical experiences, but also interact and learn about the other country and its academic-related practices.
- Leveraging on complementary research skills: the collaboration would be more effective if teams provide complementary skills and expertise, enabling a result that is larger than its constituent parts.
- Cybersecurity is a multi-cultural, multi-lingual and multi-media issue: research of cybersecurity should take into account local factors that may affect significantly the cybersecurity issues to be tackled. Thus, cooperation projects represent an opportunity for developing models, algorithms and methodologies that are able to handle such diversity.

- Gain knowledge of different regulation frameworks: Regulation frameworks vary significantly among countries and attacks often exploit regulation omissions. For instance, the Brazilian regulation is much less strict with respect to privacy, allowing improper privacy-related attacks and activities.
- Dual-environment assessment scenarios: Cooperation projects will enable the assessment of the research outcomes in different scenarios, employing different strategies that differ between countries. Local demands and attack strategies require novel cybersecurity solutions. One example scenario is the financial and banking system, since the threat motivations may be different in each country. In Brazil, a major motivation may be more related to identity theft as a way to perform online banking and credit card frauds, while in the US terrorism may be a major reason for the cybercrimes. Such assessments would allow the researchers to evaluate the generality of techniques and methodologies. Further, the access and knowledge acquisition about different markets may help future initiatives to transfer the technologies associated with research outcomes.

Opportunities For the United States:

From the perspective of American researchers and research groups, the group envisages the following opportunities while cooperating with Brazilian peers:

- Assessment of existing R&D outcomes in different contexts: cybersecurity research groups should have already researched and developed several artifacts that may benefit from an evaluation in a different scenario, which may present different attack strategies. For instance, smart meters to be marketed in Brazil need to be cheaper and more robust to attacks. Learning about Brazilian market may provide a competitive advantage not only for Brazil but for other countries that are similar to it.
- Brazilian internet usage still growing: The internet usage in Brazil has been increasing steadily at rates that reach 5% per year. Such a growth opens a new dimension for the cybersecurity research in Brazilian markets because the evaluation scenario basically become very dynamic.
- Access to well prepared and engaged students: Brazil has been supporting students abroad for decades, mainly at the graduate levels. A significant fraction of the resulting PhDs returned to Brazil, mainly to academia, where novel generations of students who are not only well prepared but familiar with American research culture are being constantly formed. We believe that these students are a key component for the success of cooperation projects.
- Access to other kinds of real data: the Brazilian regulation framework fosters explicitly the publication of all government-related data, as well as any data that may be of public interest. Such a policy represents a key enabler for a wide range of data-intensive research efforts.

Opportunities for Brazil

From the Brazilian perspective, the group envisages the following opportunities:

- Access to state of the art research and technology: a key motivation for Brazilian researchers and students is to ease the access to state of the art research and technology that may not be available in Brazil. It includes not just hardware, but also practices and expertise from American partners.
- Exchange experience for researchers and students: exchange experiences are very appealing for Brazilian students, as well as for significant fraction of researchers. Learning about another culture, working in a state-of-the-art lab and improving language skills are among the common reasons that justify such appeal.
- - US cybersecurity eco-system is much larger: considering the significant larger size of the US cybersecurity eco-system and market, cooperation projects would allow assessments and application of methods and technologies at a different scale, enabling Brazilian technologies to eventually reach the US market.