José Jair Cardoso de Santanna
University of Twente
Design and Analysis of Communication Systems (DACS)
Drienerlolaan 5, Zl-5110
7522 NB Enschede, The Netherlands

CONFIDENTIAL PERSONNEL MATTER
The Department Head of the Computer Science Department
Universität der Bundeswehr München
85577 Neubiberg, München, Germany

UNIVERSITY OF TWENTE.

José Jair Cardoso de Santanna
University of Twente
Design and Analysis of Communication Systems
Drienerlolaan 5, Zl-5110, 7522 NB Enschede
Website: http://jairsantanna.com
E-mail: j.j.santanna@utwente.nl
Phone: +31 53 4892505

October 14, 2016

To the Department Head of the Computer Science Department
The Universität der Bundeswehr München
85577 Neubiberg, Mnchen, Duitsland

Subject: *Application letter to the University Professorship (W3) in ICT Threat and Malware Analysis.*

Dear Sir or Madam,

I am writing to apply for the position of University Professorship (W3) in *ICT Threat and Malware Analysis* beginning 2018, as advertised on the Universitt der Bunderswehr Mnchen (UniBwM) website. I am currently a doctoral candidate at the University of Twente, the Netherlands, and fully expect to complete my Ph.D. degree requirements by April 2017. It was already offered me a postdoctoral position to stay in the same university after achieved the Doctor degree, which I intend to accept till I get a professorship position in a center of excellence in research. I am extremely interested in obtaining a professorship position at the UniBwM, as its Cyber Defence Research Center (CODE) promises to have a stellar reputation worldwide. I believe that my academic training, teaching and advising experience prepare me to be an effective researcher and instructor in your department.

My doctoral research is conducted under the direction of Prof. Aiko Pras, and target the investigation of a serious Cyber Threat to any system in the Internet, called Booters. Booters are websites that publicly offer Distributed Denial of Service (DDoS) attacks to-and-against anyone as a paid service. This websites are involved in most of the DDoS attacks, specially those called mega attack (greater than 100 Gb/s of traffic). Besides my multidisciplinary investigation, which includes the technical, legal, ethical and economical aspects, in my research, I developed a methodology to find the most comprehensive list of Booter websites. The outcome of this methodology is weekly updated and shared at `http://booterblacklist.com`. It was already downloaded by almost one thousand people worldwide. Additionally, I am developing one of the largest open databases with DDoS attacks traces and fingerprints (DDoSDB avaliable at `http://ddosdb.org`). Such database enables an earlier detection/mitigation and comparison of attacks. Together with DDoSDB I proposed a methodology that enable companies to share their attacks traces assuring the privacy of their clients. Among the list with dozens collaborators I highlight Booking.com, the Dutch public broadcasting system (NPO), and the Dutch National Foundation Manager of ISPs (NBIP). All the achievements during my PhD also gave me the opportunity to advise both the Japanese Ministry of Internal Affairs & Communications and the Dutch Ministry of Security & Justice on the topic of Cyber Security and DDoS attacks.

During the last couple of years I had two papers on Botnet analysis, named Kelihos.B and Carna Botnet (which produced the Internet Census 2012). I also had change to guide several bachelor students on a Honeypot assignment which investigate the operation of dozens Malwares. Beside my experience with DDoS attacks, Botnets, and Malwares, I am convinced that I can address any security problem in ICT.

My teaching experience started right after I achieved my master degree in computer science. I had the opportunity to teach for two semesters the courses Digital Systems, Computer Networks, and Network Management at the University of Santa Cruz do Sul, Brazil. In the last two years I also had the great opportunity to be guest lecturer on the topic of Cyber Security, Cyber Defense, and Network Management. I have developed confidence and passion in teaching any topic related to network security. The feedback of students/attendees [1] gives me the certainty that I have a great potential to pursue an academic career.

My advising experience. I advised in total twenty five students: five to achieve the Master degree, five to the Bachelor degree, and fifteen supporting bachelor minor assignments, such as design projects, literature studies, and honeypot assignment. I would like to highlight that: (1) half of the master and bachelor students had papers accepted in international conferences and decided to follow towards the next academic degree, (2) one got the best paper award and (3) one got a renowned Dutch national prize (KIVI/Defensie & Veiligheid). This evidences emphasis my ability to lead people towards research of excellence.

I would enjoy discussing this position with you at any moment. In the meantime, I am enclosing my Curriculum Vitae for your analysis. If you require any additional materials or information, I am happy to supply it. Thank you very much for your consideration.

Yours faithfully,

José Jair Cardoso de Santanna

[1] Voluntarily feedbacks of students/attendees are available at `http://bit.ly/presentation_evaluation`.

José Jair Cardoso de **Santanna**

Enthusiastic, Researcher, Teacher, Network Security Specialist & (Big) Data Analyst

Contact

University of Twente
DACS research group
Drienerlolaan 5
7522 NB Enschede
The Netherlands

j.j.santanna@utwente.nl
+31 53 4892505

Links

jairsantanna.com
/TxcQNxUAAAAJ
/0...2-8361-6729
/K-2169-2016
/jjcsantanna
/jjsantanna

Languages

Dutch★★☆☆☆
Spanish★★★☆☆
English★★★★★
Portuguese★★★★★

Status and Professional Objective

I am currently PhD candidate at University of Twente with a postdoctoral contract starting right after I achieve the Doctor degree (expected April 2017) in the same university. My research is founded by the European commission and by the Dutch national Organisation for Scientific Research (NWO). Some results of my research achieved recognition in the national and international level; for example, I had the opportunity to advise the Japanese Ministry of Internal Affairs and Communications and the Dutch National Cyber Security Center both on the topic of cyber security. My professional objective is to become an internationally recognized researcher and teacher in cyber security. I aim to transfer my enthusiasm, knowledge, skills and experience into meaningful innovation to improve the security in all types of networks, specially in the Internet.

Education

2013–apr/2017* **Doctor** in Computer Science — University of Twente, The Netherlands
"The Investigation of the DDoS as a Service Phenomenon".
Supervisor: Prof. Dr. Ir. Aiko Pras
This ongoing work has being used by both the security community and by network operators worldwide. One of the outcomes that stands out is publicly available at 'booterblacklist.com' and already downloaded by more than four hundred users worldwide.

2010–2012 **Master** in Computer Science — Federal University of Rio Grande do Sul, Brazil
"A BPM-based Solution for Inter-domain Circuit Management".
Supervisor: Prof. Dr. Lisandro Zambenedetti Granville
The outcome of this work is still in production used by the Brazilian National Education and Research Network and available at 'meican.cipo.rnp.br'.

2005–2010 **Bachelor** in Computer Engineer — Federal University of Pará, Brazil
"A Comparative Evaluation of DCCP Protocol in Mesh Networks."
Supervisor: Dr. Kelvin Lopes Dias

Experience

Technical Adviser

2016 **To the Yokohama National University** — Japan
For the production of a report on "Reflection & Amplification DDoS attacks" requested by the *Japanese Ministry of Internal Affairs and Communications*.

2016 **To the Dutch National Cyber Security Center and the Scientific Research & Documentation Center** — The Netherlands
For the production of a report on "Cyber metrics 2016: DDoS and Malware" requested by the *Dutch Ministry of Security and Justice*.

Assistant Professor

2012–2013 **University of Santa Cruz do Sul (UNISC)** — Santa Cruz do Sul, Brazil
Tasks & Responsibilities: Supervise students and teach (integrally) the courses:
● **Digital Systems;**
● **Computer Networks; and**
● **Network Management**.

Guest Lecturer

Most of my slides are available at slideshare.net/jjcsantanna; some interactive exercises are available at github.com/jjsantanna/lectures_hands_on; and, most important, there is some voluntary judgment and testimonies of students available at bit.ly/presentation_evaluation.

2016 **Network Management** University of Twente, The Netherlands
Lectures: (1) " SNMPv1, v2, v3 and Beyond" and (2) "Network management based on WebServices"
Audience: master students of computer science, electrical engineer, and telematics from the University of Twente.

2015 & 2016 **Product Design to Online Business** University of Twente, The Netherlands
Lectures: (1) "Booters: the DDoS-as-a-Service phenomenon" and (2) "Product Design to Online Business"
Audience: bachelor students of industrial engineering and business information technology.

2015 **Network Security** University of Twente, The Netherlands
Lecture: "DDoS attacks into the Matrix"
Audience: master and bachelor students of computer science, electrical engineer, and telematics from the University of Twente, 3TU cyber security, and members of ICT labs.

2015 **Cybercrime & Cybersecurity (minor)** University of Twente, The Netherlands
Lecture: "DDoS attacks - Back to the future"
Audience: bachelor students from University of Twente, European Research Center for Information (ERCIS), Westfälische Wilhelms - Univerität Münster, Universität Innsbruck, and University of Leicester.

Student Supervisor

Among 10 supervised students: 6 had their research published in international academic conferences, 5 decided to follow towards the next academic degree [*] (Ph.D. or M.Sc.), 2 received the M.Sc. degree cum laude [+], 1 won the best paper award in an international conference [#], 1 won the second place of a renowned Dutch national prize (KIVI/Defensie & Veiligheid) for her thesis [!], and 1 is working as Digital Expert for the Dutch National High Tech Crime Unit [§].

[**M.Sc. Degree**] Justyna Chromik[*,+,!] , Wouter de Vries[*,#], Joey de Vries[+], Mark Wierbosch, and Jarmo van Lenthe[§].

[**B.Sc. Degree**] Roeland Krak[*], Max Kerkers[*], Dirk Maan[*], Jochum Börger, and Guilherme Dressler.

Journal and Conference Reviewer

Among more than 20 venues acting as a reviewer I highlight bellow only journals (3) and the (3) top well ranked conferences by the (IEEE) Committee on Network Operation and Management (CNOM). While for journal I added the 'impact factor' and the 'h-index' metrics, for conferences the 'acceptance rate' and, also, the 'h-index', respectively.

COMCOM	**Computer Communications**	2.099 | 49
JNSM	**Journal of Network and Systems Management**	0.796 | 15
IJNM	**International Journal of Network Management**	0.681 | 10
CNSM	**International Conference on Network and Service Management**	17.6% | 18
NETWORKING	**IFIP Networking**	23.8% | 22
IM	**IFIP/IEEE Integrated Management**	27.2% | 18

Conference Organizer

2016 **Shadow Technical Program Committee (TPC)** CNSM
IFIP/IEEE International Conference on Network and Service Management is the premier conference in the area of network and service management. A shadow TPC is an experimental initiative for PhDs become better TPCs in the future. My reviews have the same weight as the actual TPC reviews.

2013-2016 **Technical Program Committee (TPC)** ERRC
Escola Regional de Redes de Computadores (pt_br), a conference for undergrad students from the south of Brazil. To motivate students to

2012 **Local Organizing Committee** LatinCloud
IEEE Latin American Conference on Cloud Computing and Communications.

2010 **Local Organizing Committee** SBRC
The Brazilian Symposium on Computer Networks and Distributed Systems.

Presentations

In the last 3 years I gave more than 30 presentations, which is almost one per month. Most of the presentations are available at 'slideshare.net/jjcsantanna'. Among invited presentations, presentations that required abstract and presentations approved after a very strict peer-reviewing process (conferences) I highlight the following.

Invited	To Logius (part of the Dutch Ministry of Interior and Kingdom Relations)	2015
Invited	To the Dutch Organization of Internet Providers (NBIP)	2015
Invited	To the Dutch National Cyber Security Centrum (NCSC)	2015
Abstract	36th IRTF Network Management Research Group (NMRG)	2015
Abstract	31th IRTF Network Management Research Group (NMRG)	2013

Rewards & Awards

2016	**Best Poster Presentation**	2nd Cyber Security Workshop in the Netherlands
2016	**Invited to the Dagstuhl Seminar 16361**	on SDN Security Challenges & Opportunities
2015	**Invited to the Dagstuhl Seminar 16012**	on Global Measurements
2015	**Best Ph.D. 'Elevator Pitch' (1st Place)**	CTIT Symposium, University of Twente
2015	**Best Poster Presentation (3rd Place)**	CTIT Symposium, University of Twente
2015	**Best Paper Award**	Autonomous Infrastructure, Management and Security Conference
2010	**Student Award (3rd Place)**	Computer Engineer, Federal University of Pará, Brazil

Scientific Appendix

Publications

DDoS 3.0 - How Terrorists Bring Down the Internet
Aiko Pras, José Jair Santanna, Jessica Steinberger, Anna Sperotto
International GI/ITG Conference, MMB & DFT (invited), 2016

Booter Blacklist: Unveiling DDoS-for-hire Websites
José Jair Santanna, Ricardo O. Schmidt, Daphner Tuncer, Joey Vries, Lisandro Granvile, Aiko Pras
International Conference on Network and Service Management (CNSM)[acceptance 17.6%], 2016

Ludo – kids playing Distributed Denial of Service
Jessica Steinberger, José Jair Santanna, Evangelos Spatharas, Hendrik Amler, Niklas Breuer, Kristian Graul, Benjamin Kuhnert, Ulrike Piontek, Anna Sperotto, Harald Baier, Aiko Pras
TERENA Networking Conference (TNC) (abstract), 2016

Booter websites characterization: Towards a list of threats
Justyna Joanna Chromik, José Jair Santanna, Anna Sperotto, Aiko Pras
Brazilian Symposium on Computer Networks and Distributed Systems (SBRC)[acceptance 30%], 2015

Inside Booters: An Analysis on Operational Databases
José Jair Santanna, Romain Durban, Anna Sperotto, Aiko Pras
IFIP/IEEE International Symposium on Integrated Network Management (IM)[acceptance 27.2%], 2015

Booters - An Analysis of DDoS-as-a-Service Attacks.
José Jair Santanna, Roland Rijswijk-Deij, Anna Sperotto, Rick Hofstede, Mark Wierbosch, Lisandro Zambenedetti Granville, Aiko Pras
IFIP/IEEE International Symposium on Integrated Network Management (IM)[acceptance 27.2%], 2015

How Asymmetric Is the Internet? A Study to Support the Use of Traceroute
Wouter Vries, José Jair Santanna, Anna Sperotto, Aiko Pras
International Conference on Autonomous Infrastructure, Management and Security (AIMS)[acceptance 31.8%], 2015

Characterisation of the Kelihos.B Botnet
Max Kerkers, José Jair Santanna, Anna Sperotto
International Conference on Autonomous Infrastructure, Management and Security (AIMS)[acceptance 31%], 2014

Towards Validation of the Internet Census 2012
Dirk Maan, José Jair Santanna, Anna Sperotto, Pieter-Tjerk Boer
EUNICE/IFIP International Workshop (EUNICE)[acceptance 47.9%], 2014

Characterizing and Mitigating The DDoS-as-a-Service Phenomenon
José Jair Santanna, Anna Sperotto
International Conference on Autonomous Infrastructure, Management and Security (AIMS)[acceptance 31%], 2014

Through the Internet of Things - A Management by Delegation Smart Object Aware System (MbDSAS)
Marcelo Marotta, Felipe Carbone, José Jair Santanna, Liane Tarouco
IEEE Computer Software and Applications Conference (COMPSAC)[acceptance 17%], 2013

Redes de Rádios Cognitivos: Arquiteturas, Sensoriamento Espectral e Questões Regulatórias.
Rafael Kunst, Cristiano Both, Lucas Bondan, Maicon Kist, José Jair Santanna, Leonardo Faganello, Lisandro Granville, Juergen Rochol
Simpósio Brasileiro de Telecomunicações (SBrT)[acceptance 18%]. 2012

A BPM-based solution for inter-domain circuit management
José Jair Santanna, Juliano Wickboldt, Lisandro Zambenedetti Granville
IEEE Network Operations and Management Symposium (NOMS)[acceptance 26.2%], 2012

Internet of Things in healthcare: Interoperatibility and security issues
Liane Tarouco, Leandro Bertholdo, Lisandro Zambenedetti Granville, Lucas Arbiza, Marcelo Marotta, José Jair Santanna
IEEE International Conference on Communications (ICC)[acceptance 37%], 2012