RÉPUBLIQUE DU CAMEROUN
REPUBLIC OF CAMEROON
Peace – Work - Fatherland

UNIVERSITÉ DE DSCHANG
UNIVERSITY OF DSCHANG
Scholae Thesaurus Dschangensis Ibi Cordum

BP 96, Dschang (Cameroun) – Tél./Fax (237) 233 45 13 811
Website : http://www.univ-dschang.org.
E-mail : udsrectorat@univ-dschang.org

FACULTE DES SCIENCES
FACULTY OF SCIENCE

Département de Mathématiques et Informatique
Department of Mathematics and Computer Science

BP 67, Dschang (Cameroun)
Tél./Fax (237) 233451735
Website : http://fs.univ-dschang.org
E-mail : dept.math-info@univ-dschang.org

Ref.N° 1656 */21/UDS/FS/D/CERVARENT/CDMI*

Dschang, le 20 AOUT 2021

Announcement

GMC-DRA project: Call for proposal for the Selection of PhD students for research in cyber-security

Within the framework of the research project "***Game Theory and Machine Learning for Cyber Deception, Resilience and Agility (GMC-DRA)***" funded by the *US Army Research Laboratory*, within URIFIA (Fundamental Computer Science, Engineering and Application Research Unit) of the Department of Mathematics and Computer Science (DMI), The Dean of the Faculty of Science (FS) of the University of Dschang (UDs) is launching a special call for the selection of fifteen (15) researchers wishing to continue their PhD research on the topic of cyber-security.

How to Apply:

- Submit an application file for registration into Year 1 according to the current criteria at the UDs Doctoral School; or be regularly registered in PhD Year 1 or PhD Year 2 at UDs (in the latter case, having produced a high-level article on the same topic is a plus);
- Provide legalized copies of all university transcripts and certificates of achievement of graduate levels; the candidate must have obtained an average greater than 12/20 in Master 1, Master 2 and possibly in PhD 1;
- Provide an updated and signed CV, highlighting the candidate's strengths;
- Provide a 5 pages research proposal written in English to be presented in English with PPT, in front of the preselection jury;
- Send a letter of motivation to the Dean of the Faculty of Science.
- The full application package in WORD or PDF should be submitted by email at
  <dept.math-info@univ-dschang.org> with cc to **<marcellin.nkenlifack@gmail.com>**
  The email subject should be "**PhD in Cyber Security**".

Note:

- This PhD call for admission is open to the best candidates from Universities in Cameroon and abroad wishing to pursue a PhD at the University of Dschang;
- Applicants should be able to **write and speak English** fluently;
- The **deadline for submitting applications is 12 September 2021**; research presentation will be scheduled right after;
- Applicants should ensure that they have carefully read the information contained in this announcement beforehand;
- The selected candidates will participate in all specialized seminars in the field, within the URIFIA of DMI;
- Selected candidates must be fully dedicated to their PhD research for 3 years and not be involved in any other activities. They will receive a monthly stipend to cover their living expense;
- Selected candidates will receive financial assistance for participation in top-tier international conferences;
- A few PhD co-tutelle will be supported under this project;
- Application from women and underrepresented group in cyber security is highly encouraged.

The Dean
Faculty of Science

RÉPUBLIQUE DU CAMEROUN Republic of Cameroon FACULTÉ DES SCIENCES Faculty of Sciences LE DOYEN UNIVERSITÉ DE DSCHANG University of Dschang

Pr Ngameni Emmanuel
professeur

Project Description

Cyber security is a serious concern to our economic prosperity and national security. Despite an increased investment in cyber defense, cyber-attackers are becoming more creative and sophisticated. Moreover, the scope and repercussions of cyber-attacks has increased over time. This exposes the need for a more rigorous approach to cyber security, including methods from artificial intelligence including game theory and machine learning. Using a game theoretic approach to cyber security is promising; however, one has to deal with many types of uncertainty such as incomplete information, imperfect information, imperfect monitoring, partial observation, limited rationality, and the computational complexity of finding equilibrium or optimum policies. On the other hand, artificial intelligence (AI) algorithms have typically been designed to optimize in a random stochastic environment. Recent advances in adversarial machine learning are promising to make AI algorithms more robust to deception and intelligent manipulation. However, they are still vulnerable to adversarial inputs, data poisoning, model stealing and evasion attacks. The above challenges and the high risk and consequence of cyber-attacks drive the need to accelerate basic research on cyber security.
The technical approaches on this project focuses on two primary areas of AI that are especially promising and relevant for cyber security: **game theory** and **machine learning**. These areas overlap to some extent, but game theory focuses more on decision making in adversarial settings, while machine learning focuses more on using large data sets for prediction and adaptation. We are also interested on a proactive cyber defense highlighting cyber deception, cyber resilience, and cyber agility or moving target defense.

Cyber deception is any attempt to disguise a network and impair the attacker's decision with false information to protect critical nodes. Deception can delay a cyber-attack by increasing uncertainty. Deception also forces the attacker to perform more trial and error in the reconnaissance phase which increases the probability of intruder detection. The use of honeypots is a basic form of cyber deception used to create the appearance of important targets to the attacker. Honeypots also help to identify attackers and provide a means to learn about their behaviors in a safe environment. The attacker's strategies learned via the use of honeypots aid in securing critical components. A honeynet is a decoy network that contains one or more honeypots. Valuable deception techniques must confuse the attacker while being transparent to the defender and legitimate users. Advanced deception techniques can dynamically hide or create fake vulnerabilities, data, protocols, communication links, hardware, software and applications. However, given enough time, an attacker may be able to discover the defender's deception strategy. Therefore, a sophisticated cyber deception technique is most often combined with cyber agility.

Cyber agility or moving target defense is the dynamic reconfiguration of network parameters, components, topology, and protocols to oppose an attacker's ability to collect information about the system. A static configuration gives enough time to attackers to learn about the system and identify potential vulnerabilities or exploits in the reconnaissance phase. An agility strategy randomly changes the attack surface and network pattern faster than an attacker can learn.

Cyber resilience refers to the network capability to continuously maintain mission essential functions after a cyber-attack. As information systems become ever more complex and the interdependence of these systems increases, defending our network becomes more and more critical. Unfortunately, it is not always possible to anticipate every type of component failure and cyber-attack within a large information system. Therefore, a mission-critical system placed in cyberspace should be resilient and have the fight-through ability to sustain damage yet survive and recover with mission assurance.

We encourage PhD proposal submission on research topic related to the following topics of interest (suggestive but not exhaustive, not in any order):

1. Game theoretic models for cyber security and privacy: [1] - [3]
2. Game theory for Cyber deception [4]- [8]
3. Cyber deception [9] - [14]
4. Attack graph modeling of cyber deception [15] - [16]
5. Epidemic model against cyber deception [17] – [18]
6. Adversarial Machine Learning [19] - [20]
7. AI for cyber deception [21]
8. Intelligent and rapid honeynet generation [22] - [23]
9. Design of high interaction honeypot [24]
10. Software Defined Network for Cyber Deception [25]–[26]

11. Location deception
12. Autonomous cyber security [27], [28]
13. Behavioral game theory for security [29] - [31], [58]
14. Planning and stochastic games for security [32]–[34]
15. Hypergames for cyber security [35]–[38]
16. Uncertainty and robustness for security [39], [59]
17. Proactive cyber defense [40]–[44]
18. Cyber agility and Moving Target Defense [44] - [45]
19. Anomaly detection [46] - [47]
20. Security aspects in Autonomous Vehicle [48]–[50]
21. Internet of Things (IoT) and Cyber Physical System (CPS) security [25], [41], [51]
22. Cyber resilience [52]–[55]
23. Novel methods to combine complementary techniques for cyber resiliency, such as game theory and machine learning [1], [6]
24. Development of agents that are doers, not just watchers: autonomy and intelligence for rapid response to a compromise and rapid recovery that aids resilience of system [56] - [57]
25. Knowledge based planning of implementation of an autonomous intelligent cyber defense agent [27] - [28]
26. Adaptive learning, development of a structured world-model, and mechanism for dealing with explicitly defined, multiple and potentially conflicting goals.

A successful proposal should address the following questions well known as DARPA Heilmeier question:

- What are you trying to do? Articulate your objectives using absolutely no jargon.
- How is it done today, and what are the limits of current practice?
- What is new in your approach and why do you think it will be successful?
- Who cares? If you are successful, what difference will it make?
- What are the risks?
- How long will it take?
- What are the mid-term and final "exams" to check for success?

Research Team:

- Pr Marcellin Nkenlifack, Head of Department of Math and Computer Science, University of Dschang
- Pr Gabriel Deugoue, Associate Professor, University of Dschang
- Dr Vianney Kengne Tchendji, Assistant Professor, University of Dschang
- Dr Elie Fute Tagne, Assistant Professor, University of Dschang
- Dr Jean Pierre Lienou Tchawe, Assistant Professor, University of Dschang

Research Collaborators:

- Dr Charles Kamhoua, Senior Electronics Engineer, US Army Research Laboratory
- Dr Frederica Nelson, Senior Computer Scientist, US Army Research Laboratory
- Dr Jaime Acosta, Senior Computer Scientist, US Army Research Laboratory
- Dr Ahmed Hemida, Postdoctoral Fellow, US Army Research Laboratory
- Dr Laurent Njilla, Research Electronics Engineer, US Air Force Research Laboratory
- Pr Yezekael Hayel, University of Avignon
- Pr Sachin Shetty, Professor, Old Dominion University
- Pr Danda Rawat, Professor, Howard University
- Pr Christophe Bobda, Professor, University of Florida
- Dr Deepak Tosh, Assistant Professor, University of Texas El Paso

References

1) C. Kamhoua, C. Kiekintveld, F. Fang, and Q. Zhu, "Game theory and machine learning for cyber security," 2021.
2) C. A. Kamhoua, L. L. Njilla, A. Kott, and S. Shetty, Modeling and design of secure internet of things. John Wiley & Sons, 2020.
3) Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, Sundaraja Sitharama Iyengar "Game Theory for Cyber Security and Privacy" ACM Computing Surveys (CSUR), Volume 50, Issue 2, Article No. 30, June 2017.
4) Zheyuan Ryan Shi, Ariel D. Procaccia, Kevin S. Chan, Sridhar Venkatesan, Noam Ben-Asher, Nandi O. Leslie, Charles A. Kamhoua, Fei Fang "Learning and Planning in Feature Deception Games" in the proceedings of the Conference on Decision and Game Theory for Security (GameSec 2020), College Park, USA, October 2020.

5) J. Pawlick, E. Colbert, Q. Zhu "A game-theoretic taxonomy and survey of defensive deception for cybersecurity and privacy" ACM Computing Surveys (CSUR), 2019.
6) M. Zhu, A. H. Anwar, Z. Wan, J.-H. Cho, C. Kamhoua, and M. P. Singh, "A survey of defensive deception: Approaches using game theory and machine learning," IEEE Communications Surveys & Tutorials, 2021.
7) Anjon Basak, Sridhar Venkatesan, Marcus Gutierrez, Ahmed Hemida, Charles A. Kamhoua, Christopher Kiekintveld "Identifying Stealthy Attackers in a Game Theoretic Framework Using Deception" in the proceedings of the Conference on Decision and Game Theory for Security (GameSec 2019), Stockholm, Sweden, October 2019.
8) Aliou Badra Sarr, Ahmed H. Anwar, Nandi O. Leslie, Charles A. Kamhoua, Jaime C. Acosta "Software diversity for cyber deception" in the proceedings of the 2020 IEEE Global Communications Conference (IEEE GLOBECOM), Taipei, Taiwan, December 2020.
9) MD Ali Reza Al Amin, Sachin Shetty, Laurent Njilla, Deepak Tosh, Charles A. Kamhoua "Hidden Markov Model and Cyber Deception for the Prevention of Adversarial Lateral Movement" IEEE Access, In press.
10) MD Ali Reza Al Amin, Sachin Shetty, Laurent Njilla, Deepak Tosh, Charles A. Kamhoua "Attacker Capability based Dynamic Deception Model for Large-Scale Networks" EAI Endorsed Transactions on Security and Safety, in press.
11) Md Ali Reza Al Amin, Sachin Shetty, Laurent Njilla, Deepak K Tosh, Charles A. Kamhoua "Online Cyber Deception System using Partially Observable Monte-Carlo Planning Framework" in the proceedings of the 15th International Conference on Security and Privacy in Communication Networks (SecureComm 2019), Orlando, FL, October 2019.
12) J. C. Acosta, A. Basak, C. Kiekintveld, N. Leslie, and C. Kamhoua, "Cybersecurity deception experimentation system," in 2020 IEEE Secure Development (SecDev). IEEE, 2020, pp. 34–40.
13) Jaime C. Acosta, Anjon Basak, Christopher Kiekintveld, Charles A. Kamhoua "Lightweight On-demand Honeypot Deployment for Cyber Deception" The 12th EAI International Conference on Digital Forensics & Cyber Crime (EAI ICDF2C), Singapore, December 2021.
14) Luan Pham, Massimiliano Albanese, Ritu Chadha, Cho-Yu Jason Chiang, Sridhar Venkatesan, Charles A. Kamhoua, Nandi Leslie "A Quantitative Framework to Model Reconnaissance by Stealthy Attackers and Support Deception-Based Defenses" in the proceedings of the IEEE Conference on Communications and Network Security (CNS) 2020, Avignon France, June 2020.
15) S. Milani, W. Shen, K. S. Chan, S. Venkatesan, N. O. Leslie, C. Kamhoua, and F. Fang, "Harnessing the power of deception in attack graph-based security games," in Decision and Game Theory for Security: 11th International Conference, GameSec 2020, College Park, MD, USA, October 28–30, 2020, Proceedings, vol. 12513. Springer Nature, 2020, p. 147.
16) A. H. Anwar and C. Kamhoua, "Game theory on attack graph for cyber deception," in International Conference on Decision and Game Theory for Security. Springer, 2020, pp. 445–456.
17) O. Tsemogne, Y. Hayel, C. Kamhoua, and G. Deugou´e, "Game theoretic modeling of cyber deception against epidemic botnets in internet of things," IEEE Internet of Things Journal, 2021.
18) Olivier Tsemogne, Yezekael Hayel, Charles A. Kamhoua, Gabriel Deugoue "Partially Observable Stochastic Games for Cyber Deception against Network Epidemic" in the proceedings of the Conference on Decision and Game Theory for Security (GameSec 2020), College Park, USA, October 2020.
19) S. Y. Khamaiseh, I. Alsmadi, and A. Al-Alai, "Deceiving machine learning-based saturation attack detection systems in sdn," in 2020 IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN). IEEE, 2020, pp. 44–50.
20) L. Huang, A. D. Joseph, B. Nelson, B. I. Rubinstein, and J. D. Tygar, "Adversarial machine learning," in Proceedings of the 4th ACM workshop on Security and artificial intelligence, 2011, pp. 43–58.
21) S. Fugate and K. Ferguson-Walter, "Artificial intelligence and game theory models for defending critical networks with cyber deception," AI Magazine, vol. 40, no. 1, pp. 49–62, 2019.
22) A. Capalik, "Next-generation honeynet technology with real-time forensics for us defense," in MILCOM 2007-IEEE Military Communications Conference. IEEE, 2007, pp. 1–7.
23) L. Spitzner, "The honeynet project: Trapping the hackers," IEEE Security & Privacy, vol. 1, no. 2, pp. 15–23, 2003.
24) A. Almutairi, D. Parish, and R. Phan, "Survey of high interaction honeypot tools: Merits and shortcomings," in Proceedings of the 13th Annual PostGraduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting, PGNet2012. PGNet, 2012.
25) K. Hasan, S. Shetty, A. Hassanzadeh, M. B. Salem, and J. Chen, "Software-defined networking for cyber resilience in industrial internet of things (iiot)," Modeling and Design of Secure Internet of Things, pp. 453–477, 2020.
26) E. Molina and E. Jacob, "Software-defined networking in cyber-physical systems: A survey," Computers & electrical engineering, vol. 66, pp. 407–419, 2018.
27) P. Theron and A. Kott, "When autonomous intelligent goodware will fight autonomous intelligent malware: A possible future of cyber defense," in MILCOM 2019-2019 IEEE Military Communications Conference (MILCOM). IEEE, 2019, pp. 1–7.
28) A. Kott, P. Th´eron, M. Dra˘sar, E. Dushku, B. LeBlanc, P. Losiewicz, A. Guarino, L. Mancini, A. Panico, M. Pihelgas et al., "Autonomous intelligent cyber-defense agent (aica) reference architecture. release 2.0," arXiv preprint arXiv:1803.10664, 2018.
29) C. Gonzalez, "From individual decisions from experience to behavioral game theory: lessons for cybersecurity," in Moving target defense II. Springer, 2013, pp. 73–86.
30) Satyaki Nan, Swastik Brahma, Charles A. Kamhoua, Nandi Leslie, "Behavioral Cyber Deception: A Game and Prospect Theoretic Approach" in the proceedings of the IEEE Global Communications Conference: Communication & Information Systems Security (GLOBECOM 2019), Waikoloa, Hawaii, December 2019.

31) C. F. Camerer, "Progress in behavioral game theory," Journal of economic perspectives, vol. 11, no. 4, pp. 167–188, 1997.
32) K. Horak, B. Bosansky, P. Tomasek, C. Kiekintveld, and C. Kamhoua, "Optimizing honeypot strategies against dynamic lateral movement using partially observable stochastic games," Computers & Security, vol. 87, p. 101579, 2019.
33) Y. Guo, Y. Gong, L. L. Njilla, and C. A. Kamhoua, "A stochastic game approach to cyber-physical security with applications to smart grid," in IEEE INFOCOM 2018-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS). IEEE, 2018, pp. 33–38.
34) K. C. Nguyen, T. Alpcan, and T. Basar, "Stochastic games for security in networks with interdependent nodes," in 2009 International Conference on Game Theory for Networks. IEEE, 2009, pp. 697–703.
35) Z. Wan, J.-H. Cho, M. Zhu, A. H. Anwar, C. Kamhoua, and M. P. Singh, "Foureye: Defensive deception based on hypergame theory against advanced persistent threats," arXiv preprint arXiv:2101.02863, 2021.
36) A. N. Kulkarni, H. Luo, N. O. Leslie, C. A. Kamhoua, and J. Fu, "Deceptive labeling: hypergames on graphs for stealthy deception," IEEE Control Systems Letters, vol. 5, no. 3, pp. 977–982, 2020.
37) B. Xi and C. A. Kamhoua, "A hypergame-based defense strategy toward cyber deception in internet of battlefield things (iobt)," Modeling and Design of Secure Internet of Things, pp. 59–77, 2020.
38) J.-H. Cho, M. Zhu, and M. Singh, "Modeling and analysis of deception games based on hypergame theory," in Autonomous Cyber Deception. Springer, 2019, pp. 49–74.
39) G. Costikyan, Uncertainty in games. Mit Press, 2013.
40) Q. Yu, Z. Zhang, and J. Dofe, "Proactive defense against security threats on iot hardware," Modeling and Design of Secure Internet of Things, pp. 407–433, 2020.
41) M. Ge, J.-H. Cho, B. Ishfaq, and D. S. Kim, "Modeling and analysis of integrated proactive defense mechanisms for internet of things," Modeling and Design of Secure Internet of Things, pp. 217–247, 2020.
42) S. Xu, "Cybersecurity dynamics: A foundation for the science of cybersecurity," in Proactive and dynamic network defense. Springer, 2019, pp. 1–31.
43) R. Colbaugh and K. Glass, "Proactive defense for evolving cyber threats," in Proceedings of 2011 IEEE International Conference on Intelligence and Security Informatics. IEEE, 2011, pp. 125–130.
44) J.-H. Cho, D. P. Sharma, H. Alavizadeh, S. Yoon, N. Ben-Asher, T. J. Moore, D. S. Kim, H. Lim, and F. F. Nelson, "Toward proactive, adaptive defense: A survey on moving target defense," IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 709–745, 2020.
45) J. D. Mireles, E. Ficke, J.-H. Cho, P. Hurley, and S. Xu, "Metrics towards measuring cyber agility," IEEE Transactions on Information Forensics and Security, vol. 14, no. 12, pp. 3217–3232, 2019.
46) R. Chalapathy and S. Chawla, "Deep learning for anomaly detection: A survey," arXiv preprint arXiv:1901.03407, 2019.
47) M. Ahmed, A. N. Mahmood, and J. Hu, "A survey of network anomaly detection techniques," Journal of Network and Computer Applications, vol. 60, pp. 19–31, 2016.
48) A. Chattopadhyay, K.-Y. Lam, and Y. Tavva, "Autonomous vehicle: Security by design," IEEE Transactions on Intelligent Transportation Systems, 2020.
49) T. Litman, Autonomous vehicle implementation predictions. Victoria Transport Policy Institute Victoria, Canada, 2017.
50) M. Raya and J.-P. Hubaux, "Security aspects of inter-vehicle communications," in 5th Swiss Transport Research Conference (STRC), no. CONF, 2005.
51) D. Mendez Mena, I. Papapanagiotou, and B. Yang, "Internet of things: Survey on security," Information Security Journal: A Global Perspective, vol. 27, no. 3, pp. 162–182, 2018.
52) I. Linkov and A. Kott, "Fundamental concepts of cyber resilience: Introduction and overview," in Cyber resilience of systems and networks. Springer, 2019, pp. 1–25.
53) S. Galaitsi, B. D. Trump, and I. Linkov, "Governance for the internet of things: Striving toward resilience," Modeling and Design of Secure Internet of Things, pp. 371–381, 2020.
54) A. Kott, B. Blakely, D. Henshel, G. Wehner, J. Rowell, N. Evans, L. Mu˜noz-Gonz´alez, N. Leslie, D. W. French, D. Woodard et al., "Approaches to enhancing cyber resilience: report of the north atlantic treaty organization (nato) workshop ist-153," arXiv preprint arXiv:1804.07651,2018.
55) F. Bj¨orck, M. Henkel, J. Stirna, and J. Zdravkovic, "Cyber resilience– fundamentals for a definition," in New contributions in information systems and technologies. Springer, 2015, pp. 311–316.
56) S. Berenjian, M. Shajari, N. Farshid, and M. Hatamian, "Intelligent automated intrusion response system based on fuzzy decision making and risk assessment," in 2016 IEEE 8th International Conference on Intelligent Systems (IS), 2016, pp. 709–714.
57) P. Thorat, S. Singh, A. Bhat, V. L. Narasimhan, and G. Jain, "Sdnenabled iot: ensuring reliability in iot networks through software defined networks," in Towards Cognitive IoT Networks. Springer, 2020, pp. 33–53.
58) Azanguezet Quimatio, B.M., Tsognong, F. HOrBAC Optimization Based on Suspicious Behavior Detection Using Information Theory. Springer Nature – Computer Science 2, 121 (2021). https://doi.org/10.1007/s42979-021-00515-w
59) Kouam Kamdem I.G., Nkenlifack M.J.A. (2021) Data Security in Health Systems: Case of Cameroon. In: Arai K. (eds) Intelligent Computing. Lecture Notes in Networks and Systems, vol 285. pp 48-57. Springer, Cham. https://doi.org/10.1007/978-3-030-80129-8_4

RÉPUBLIQUE DU CAMEROUN
REPUBLIC OF CAMEROON
Peace – Work - Fatherland

UNIVERSITÉ DE DSCHANG
UNIVERSITY OF DSCHANG
Scholae Thesaurus Dschangensis Ibi Cordum

BP 96, Dschang (Cameroun) – Tél./Fax (237) 233 45 13 811
Website : http://www.univ-dschang.org.
E-mail : udsrectorat@univ-dschang.org

FACULTE DES SCIENCES
FACULTY OF SCIENCE

Département de Mathématiques et Informatique
Department of Mathematics and Computer Science

BP 67, Dschang (Cameroun)
Tél./Fax (237) 233451735
Website : http://fs.univ-dschang.org
E-mail : dept.math-info@univ-dschang.org

Ref.N° 1656 /21/UDS/FS/D/CERVARENT/CDMI

Dschang, le 20 AOUT 2021

Communiqué

Projet GMC-DRA : Appel à candidatures pour la Sélection de Doctorants pour les recherches avancées en cyber-sécurité

Dans le cadre du projet de recherche « **Game Theory and Machine Learning for Cyber Deception, Resilience and Agility (GMC-DRA)** » financé par « **l'US Army Research Laboratory** », au sein de l'URIFIA (Unité de Recherche en Informatique Fondamentale, Ingénierie et Applications) du Département de Mathématiques et Informatique (DMI), le Doyen de la Faculté des Sciences (FS) de l'Université de Dschang (UDs) lance un appel à candidatures pour la sélection de quinze (15) chercheurs désirant poursuivre leurs travaux de recherche en Doctorat/PhD sur cette thématique de la cyber-sécurité.

Conditions de candidature :

- Déposer un dossier de candidature pour l'inscription en première année de Doctorat (D1) selon les critères en vigueur à l'école doctorale de l'UDs ; ou être régulièrement inscrit en D1 ou en D2 à l'UDs (dans ce dernier cas, avoir produit un article de haut niveau dans la même thématique est un atout considérable) ;
- Fournir des copies légalisées des relevés de notes et attestations de réussite des niveaux universitaires ; le candidat doit avoir obtenu plus de 12/20 de moyenne en Master 1, en Master 2 et éventuellement en D1 ;
- Fournir un CV actualisé et signé, mettant en évidence les points forts du candidat ;
- Fournir une synthèse du projet/proposition de recherche sur 5 pages rédigées en Anglais à présenter en Anglais (avec PPT), devant le jury de présélection ;
- Adresser une lettre de motivation à Monsieur le Doyen de la Faculté des Sciences ;
- Le dossier de candidature complet au format WORD ou PDF doit être soumis par courrier électronique à l'adresse **<dept.math-info@univ-dschang.org>** avec cc à **<marcellin.nkenlifack@gmail.com>**
  L'objet de l'e-mail doit être « **PhD in Cyber Security** ».

NB:

- Cet appel à candidatures est ouvert aux meilleurs candidats des Universités du Cameroun et de l'étranger désirant poursuivre en cycle de Doctorat/PhD à l'Université de Dschang ;
- Les candidats doivent être capables d'écrire et de **parler couramment l'anglais** ;
- La **date limite de dépôt des candidatures est le 12 septembre 2021** ; la présentation des projets de recherche sera programmée juste après;
- Les candidats doivent s'assurer d'avoir lu attentivement les informations contenues dans cette annonce au préalable ;
- Les candidats retenus participeront à tous les séminaires spécialisés dans le domaine, au sein de l'URIFIA du DMI ;
- Les candidats sélectionnés seront entièrement dédiés à leur recherche doctorale pendant 3 ans et ne peuvent donc pas être impliqués dans d'autres activités (les travailleurs sont exclus). Ils recevront une allocation mensuelle pour couvrir leurs frais de subsistance ;
- Les candidats sélectionnés recevront également une aide financière pour participer à des conférences internationales de haut niveau ;
- Un certain nombre de cotutelles doctorales seront soutenues dans le cadre de ce projet ;
- Les candidatures de femmes et de groupes sous-représentés dans le domaine de la cybersécurité sont fortement encouragées.

Le Doyen

RÉPUBLIQUE DU CAMEROUN Republic of Cameroon FACULTÉ DES SCIENCES Faculty of Sciences LE DOYEN University UNIVERSITÉ Dschang DSCHANG

Ngameni Emmanuel
professeur