

Curriculum Vitae resumido

Paulo Lício de Geus

1 Formação

Ano	Título ou atividade	Instituição
1979	Graduação: Engenheiro Eletricista Eletrônico	FEE-UNICAMP
1985	Mestrado: Engenharia Elétrica	FEE-UNICAMP
1990	Doutorado em Ciência da Computação	University of Manchester UK
2004	Livre Docência	IC-Unicamp

2 Histórico profissional, serviços, distinções acadêmicas e prêmios

- PHT Sistemas Eletrônicos S.A. (Promon), **Engenheiro de desenvolvimento**, nov/1981–set/1985.
- DCC-IMECC-Unicamp, **Professor Instrutor**, tempo parcial, categoria MS-1, ago/1984–dez/1985
- DCC-IMECC-Unicamp, **Professor Assistente**, tempo integral, categoria MS-2, dez/1985–ago/1990
- DCC-IMECC-Unicamp, **Professor Assistente Doutor**, tempo integral, categoria MS-3, ago/1990–jan/2005
- IC-Unicamp, **Professor Associado**, tempo integral, categoria MS-5.1, fev/2005–presente
- Administrador da Rede Unix do IC-Unicamp, 1990–1996
- Membro da equipe encarregada de investigar a pane no painel da Câmara dos Deputados (Câmara Federal), por ocasião da votação das mudanças da CLT, 30/nov–02/dez/2001
- Membro da Comissão de Avaliação do Sistema Informatizado de Eleições, designada pelo Ofício UNICAMP GR 478/2001 de 13/12/2001, referente ao contrato TSE nº 54/2001, no período 12/2001–05/2002
- Librix: Desenvolvimento de Distribuição Linux para o Mercado Corporativo, convênio Itautec 2005–2011
- Consultor no Projeto “Segurança em Internet Banking” com o Banco do Brasil, abr/2011–2013
- Coordenador de pós-graduação do IC-Unicamp, jul/2011–jul/2015
- Melhor artigo, SSI’99, Keesje Duarte Pouw e Paulo Lício de Geus, “Desenvolvendo Aplicações Seguras em Ambiente HTML/HTTPS”
- Menção honrosa, SSI’01, Marcelo Abdalla dos Reis e Paulo Lício de Geus, “Forense computacional: procedimentos e padrões”
- Menção honrosa, SBSeg’05, João Porto de Albuquerque, Holger Isenberg, Heiko Krumm e Paulo Lício de Geus, “Gerenciamento Baseado em Modelos da Configuração de Sistemas de Segurança em Redes de Larga Escala”
- Melhor artigo, WTICG, SBSeg’11, Alexandre Or Cansian Baruque, André Ricardo Abed Grégio e Paulo Lício de Geus, “Análise Visual de Comportamento de Código Malicioso”
- Menção honrosa do WTICG do SBSeg’14, Victor Furuse Martins, André Ricardo Abed Grégio, Vitor Monte Afonso e Paulo Lício de Geus, “Esteno: Uma Abordagem para Detecção Visual de Bankers”
- Menção honrosa do CTDSeg do SBSeg’14, André Ricardo Abed Grégio, Paulo Lício de Geus e Mário Jino, “Malware behavior”
- Assessor da Pró-Reitoria de Desenvolvimento Universitário da Unicamp, set/2015–presente

3 Resultados de pesquisa

1. Emílio Tissato Nakamura e Paulo Lício de Geus, “Segurança de redes em ambientes cooperativos”, 1a. ed., Editora Berkeley/Siciliano, SP, 2002, ISBN 85-7251-609-3, 2a. ed., Editora Futura/Siciliano, SP, 2003, ISBN 85-7413-179-2, 3a. ed., Editora Novatec, SP, 2007, ISBN 978-85-7522-136-5, citações: 119
2. Fabrício Sérgio de Paula, Leandro Nunes de Castro and Paulo Lício de Geus, “An IDS using ideas from the immune system”, CEC’04, IEEE Congress on Evolutionary Computation, Portland, Oregon, USA, 19–23/06/2004, pp. 1059–1066, citações: 40
3. João Porto de Albuquerque, Heiko Krumm and Paulo Lício de Geus, “Policy Modeling and Refinement for Network Security Systems”, POLICY’2005, IEEE 6th International Workshop on Policies for Distributed Systems and Networks, Stockholm, Sweden, 6–8/06/2005, pp. 24–33, citações: 39
4. João Porto de Albuquerque, Heiko Krumm and Paulo Lício de Geus, “Formal Validation of Automated Policy Refinement in the Management of Network Security Systems”, International Journal of Information Security, 9(2), 99–125, Apr/2010. DOI: 10.1007/s10207-010-0101-6, citações: 8
5. João Porto de Albuquerque, Heiko Krumm, Paulo Lício de Geus and René Jeruschkat, “Scalable model-based configuration management of security services in complex enterprise networks”, Software: Practice and Experience, 41(3), 307–338, 2011. DOI: 10.1002/spe.1014, citações: 2
- 4 André R. A. Grégio, Dario S. Fernandes Filho, Vitor M. Afonso, Rafael D. C. Santos, Mario Jino and Paulo L. de Geus, “Behavioral analysis of malicious code through network traffic and system call monitoring”, SPIE’2011 Defense, Security and Sensing - Evolutionary and Bio-Inspired Computation: Theory and Applications V, Orlando, FL, USA, Proc. SPIE 8059, 80590O (2011); DOI:10.1117/12.883457, 25–29/04/2011, citações: 7
6. André Ricardo Abed Grégio, Paulo Lício de Geus, Christopher Kruegel and Giovanni Vigna, “Tracking Memory Writes for Malware Classification and Code Reuse Identification”, DIMVA’2012, the 9th Conference on Detection of Intrusions and Malware & Vulnerability Assessment, Heraklion, Crete, Greece, 26–27/07/2012, in Lecture Notes in Computer Science, v. 7591, 2013, DOI:10.1007/978-3-642-37300-8_8, pp. 134–143, citações: 0
7. André Ricardo Abed Grégio, Vitor Monte Afonso, Victor Furuse Martins, Dario Simões Fernandes Filho, Paulo Lício de Geus, Mario Jino, “An Empirical Analysis of Malicious Internet Banking Software Behavior”, SAC’2013, the 28th Annual ACM Symposium on Applied Computing, Coimbra, Portugal, 18–22/03/2013, vol. 2, pp. 1830–1835, citações: 4
8. Vitor Monte Afonso, Matheus Fávero de Amorim, André Ricardo Abed Grégio, Glauco Barroso Junquera and Paulo Lício de Geus, “Identifying Android malware using dynamically obtained features”, Journal of Computer Virology and Hacking Techniques, 11:9–17, 2015. DOI: 10.1007/s11416-014-0226-7, citações: 3
9. André Ricardo Abed Grégio, Vitor Monte Afonso, Dario Simões Fernandes Filho, Paulo Lício de Geus and Mario Jino, “Toward a Taxonomy of Malware Behaviors”, The Computer Journal, 58(10):2758–2777, 2015. DOI: 10.1093/comjnl/bxv047, citações: 0
10. Vitor Monte Afonso, Antonio Bianchi, Yanick Fratantonio, Adam Doupe, Mario Polino, Paulo Lício de Geus, Giovanni Vigna and Christopher Kruegel, “Going Native: Using a Large-Scale Analysis of Android Apps to Create a Practical Native-Code Sandboxing Policy”, NDSS’2016, the Network and Distributed System Security Symposium, San Diego, CA, USA, 21–24/02/2016, pp. 1–14

O livro “Segurança de redes...” vendeu mais de 12 mil exemplares em 13 anos, usado como livro texto Brasil afora. O mestrado de Marcelo Lima resultou em módulo oficial do kernel Linux 2.2 em diante. O trabalho de André Grégio e outros resultou em patente depositada no INPI no. BR1020130309419 em 2013. Citações: Google Scholar em 04/mai/2014.

4 Financiamentos à pesquisa vigentes

Nada a declarar.

5 Orientações em andamento

5.1 Doutorado

1. Gabriel Dieterich Cavalcante, “Uso interativo de técnicas de visualização para fins de segurança e forense computacional”, mar/2010
2. Vitor Monte Afonso, “Segurança em ambientes móveis”, bolsas CAPES e Samsung, ago/2011
3. Dario Simões Fernandes Filho, “Análise Comportamental de Malware”, bolsa Capes, ago/2011
4. Marcelo Invert Palma Salas, “Análise de malware em ambientes móveis”, bolsas CAPES e Samsung, mar/2012

5.2 Mestrado

1. Adriano Ricardo Ruggero, “Análise de Aplicações Java Visando a Identificação de Comportamento Malicioso”, bolsa CAPES, mar/2013
2. Otávio Augusto Araújo Silva, “Um esquema para proteção de dados sensíveis por meio de contenção e isolamento de processos arbitrários”, bolsa CAPES, mar/2013
3. Mayk Choji, “IDS para ambientes de Cloud”, bolsa CAPES, mar/2014
4. Bruno da Silva Melo, “Segurança em Internet of Things”, CAPES, mar/2015
5. Cicero Silva Luiz Junior, “Segurança e Privacidade em Windows”, mar/2015
6. Marcus Felipe Botacin, “Técnicas de análise comportamental de malware”, CAPES, ago/2015–
7. Victor Furuse Martins, “Advanced Persistent Threats”, ago/2015

5.2.1 Iniciação científica

1. Alexandre Or Cansian Baruque, “Análise de malware”, set/2014–
2. Beatriz Sechin Zazulla, “Métodos alternativos de autenticação”, set/2014–

6 Indicadores quantitativos

Livros (inclui edições do mesmo livro)	3
Periódicos	8
Capítulos de livros	1
Artigos em conferências	108
Orientações mestrado defendidas	33
Orientações doutorado defendidas	5
Citações Google Scholar em 27/nov/2015	410

7 Links para citações

- <http://scholar.google.com.br/citations?user=XKOLjgUAAAAJ>