Devashish Gosain

✉ *dgosain@esat.kuleuven.be*

Current Employment

2022– **Postdoctoral Researcher**, *COSIC, KU Leuven*, Belgium, (hosted by Claudia Diaz).

Past Employment

2020–2022 **Postdoctoral Researcher**, *Max Planck Institute of Informatics*, Germany, (hosted by Anja Feldmann).

Education

2015–2020 **PhD**, *IIIT-Delhi*, India.

2013-2015 **Master of Technology**, *Birla Institute of Technology*, Ranchi, India.

2008-2012 **Bachelor of Technology**, *Guru Gobind Singh Indraprastha University*, Delhi, India.

Research Interests

Networks, Privacy, anonymity, (anti-)censorship, Internet measurements.

Selected Publications

2023 **DeeP4R: Deep Packet Inspection in P4 using Packet Recirculation**, *accepted for the publication in proceedings of International Conference on Computer Communications (**INFOCOM**)*.
Authors:Sahil Gupta, **Devashish Gosain**, M Kwon, HB Acharya

2023 **On the Anonymity of Peer-To-Peer Network Anonymity Schemes Used by Cryptocurrencies**, *accepted for publication in proceedings of Network and Distributed Security Symposium (**NDSS**)*.
Authors: Piyush Kumar Sharma, **Devashish Gosain**, Claudia Diaz

2022 **Automatic Detection of Fake Key Attacks in Secure Messaging**, *in proceedings of Conference on Computer and Communications Security (**CCS**)*.
Authors:Tarun Kumar Yadav, **Devashish Gosain**, Amir Herzberg, Daniel Zappala, Kent Seamons

2021 **MiXiM: Mixnet design decisions and empirical evaluation**, *in proceedings of Workshop on Privacy in the Electronic Society (**WPES**)*.
Authors:Iness Ben Guirat, **Devashish Gosain**, Claudia Diaz

2021 **Simple Deep Packet Inspection with P4**, *demo paper in proceedings of International Conference on Network Protocols (**ICNP**)*.
Authors:Sahil Gupta, **Devashish Gosain**, G Grigoryan, M Kwon, HB Acharya

2021 **Telemetron: Measuring Network Capacity Between Off-Path Remote Hosts**, *in proceedings of Local Computer Networks (**LCN**)*.
Authors:**Devashish Gosain**, Aishwarya Jaiswal, H. B. Acharya, Sambuddho Chakravarty

2021 **Camoufler: Accessing The Censored Web By Utilizing Instant Messaging Channels**, *in proceedings of ASIA Conference on Computer and Communications Security (**AsiaCCS**)*.
Authors:Piyush Kumar Sharma, **Devashish Gosain**, Sambuddho Chakravarty

2021 **Too Close for Comfort: Morasses of (Anti-)Censorship in the Era of CDNs**, *in proceedings of Privacy Enhancing Technologies (**PoPETS**)*.
Authors:**Devashish Gosain**, Mayank Mohindra, Sambuddho Chakravarty

2020 **Maginot Lines and Tourniquets: On the Defendability of National Cyberspace**, *in proceedings of Local Computer Networks Symposium (**LCN**)*.
Authors: **Devashish Gosain**, Madhur Rawat, Piyush Kumar Sharma, H.B. Acharya

2020 **SiegeBreaker: An SDN Based Practical Decoy Routing System**, *in proceedings of Privacy Enhancing Technologies (**PoPETS**)*.
Authors: Piyush Kumar Sharma, **Devashish Gosain**, Himanshu Sagar, Chaitanya Kumar, Aneesh Dogra, Vinayak Naik, H.B. Acharya, Sambuddho Chakravarty

2019 **CAMP: cluster aided multi-path routing protocol for wireless sensor networks**, *in Wireless Networks, Springer*.
Authors: Mohit Sajwan, **Devashish Gosain**, Ajay. K. Sharma

2018 **Where The Light Gets In: Analyzing Web Censorship Mechanisms in India**, *in proceedings of Internet Measurement Conference (**IMC**)*.
Authors: Tarun Kumar Yadav*, Akshat Sinha*, **Devashish Gosain***, Piyush Sharma, Sambuddho Chakravarty. (*All authors have equal contributions.)

2018 **Hybrid energy-efficient multi-path routing for wireless sensor networks**, *in Journal of Computers and Electrical Engineering, Elsevier*.
Authors: Mohit Sajwan, **Devashish Gosain**, Ajay. K. Sharma

2017 **The Devil's in The Details: Placing Decoy Routers in the Internet**, *in proceedings of Annual Computer Security Applications Conference (**ACSAC**)*.
Authors: **Devashish Gosain**, Anshika Aggarwal, H. B. Acharya and Sambuddho Chakravarty

2017 **Mending Wall: On the Implementation of Censorship in India (Best Student Paper)**, *in proceedings of EAI International Conference on Security and Privacy in Communication Networks (**SECURECOMM**)*.
Authors: **Devashish Gosain**, Anshika Aggarwal, Sahil Shekhawat, H. B. Acharya and Sambuddho Chakravarty

2017 **Few Throats to Choke: On the Current Structure of the Internet**, *in proceedings of Local Computer Networks (**LCN**)*.
Authors: H. B. Acharya*, Sambuddho Chakravarty* and **Devashish Gosain***. (*All authors have equal contributions.)

2017 **DSERR: Delay Sensitive Energy Efficient Reliable Routing Algorithm for wireless sensor networks**, *in Wireless Personal Communication (WPC), Springer*.
Authors: **Devashish Gosain**, Itu Snigdh, Mohit Sajwan

2016 **Analysis of scalability for routing protocols in wireless sensor networks**, *Optik-International Journal for Light and Electron Optics, Elsevier*.
Authors: **Devashish Gosain**, Itu Snigdh

Selected Ongoing Research Projects

Behind the Curtain: The New Order of Internet Censorship in India.
We study a new form of Internet censorship i.e., mobile app blocking and describe in detail the mechanics involved. We study 220 Chinese apps that were recently blocked in India. We observed a novel "three-tiered" app censorship scheme in India, with each tier increasing the sophistication of censorship. After thoroughly analyzing the app censorship mechanisms, we present effective circumvention techniques to bypass the tiered app censorship. We were able to access all the blocked apps with the said techniques.

A Multi-Perspective Analysis of Web Cookies.
We conducted a comprehensive measurement study to analyze the cookie differences (for Tranco top-10k websites) from geographically diverse locations and report the impact of such factors. Specifically, we study the cookie differences (1) before and after interacting with cookie banners (2) between landing and inner pages of a given website. We statistically test how consistent are websites with respect to the cookies they send. Additionally, we also report cookie differences for CCPA compliant websites when accessed from California and the rest of the world. Our study highlights that the said factors significantly impact the cookie landscape and thus must be considered while performing measurement studies.

Friend or Foe: Onion Routing and Cryptocurrencies.
In this research, we performed a series of active and passive measurements collecting data about the Bitcoin network. For the passive analysis, we collected the Bitcoin network snapshots (from the Bitnodes project) and reported that there had been significant growth in onion addresses since 2020. Currently, the number of onion addresses is more than the IP addresses in the Bitcoin network. We also measured the churn and reachability of onion addresses. We found that although onion addresses have high daily churn, but they occur relatively more often than IP addresses in longer time frames (e.g., a month). Moreover, we demonstrated that onion addresses could facilitate partitioning attacks by bringing down the cost required to perform the attack from access to a tier-1 AS (assumed in the latest partitioning attack) to the control of about 1000 cloud hosts. Through extensive simulations, we showed that the attack was successful in different test scenarios.

Teaching

2023 **Lecturer of Advanced Privacy Technologies at KU Leuven**.

2022 **Teaching Assistant**, *KU Leuven*.
Privacy and Big Data

2022 **Teaching Assistant**, *KU Leuven*.
Privacy Technologies

2022 **Co-Lecturer of Data Networks course at Saarland University** , *(with Anja Feldmann, Oliver Gasser, Yiting Xia and Jialong Li)*.

2021 **Co-Lecturer of Data Networks course at Saarland University** , *(with Anja Feldmann, Oliver Gasser, and Savvas Zannettou)*.

2015 - 2020 **Teaching Assistant**, *IIIT-Delhi*.
Secure Coding, Network Security, Software Defined Networks, Scientific Communication, Security Engineering

Research Internships

Sept. 2019 - Dec. 2019 **Visiting Scholar**, *Brigham Young University*, Utah, USA.
Automatic Detection and Prevention of Fake Key Attacks in Secure Messaging.
Popular IM applications *e.g.,* WhatsApp provide end-to-end encryption for billions of users. Designed several defenses for fake key attacks and use a threat analysis to identify which attacks each defense can automatically detect or prevent.

Invited Talks

Feb. 2020 **Internet Maps and Censorship**, *COSIC, KU Leuven*, Belgium.

Services

2022 **PC member**, *European Symposium on Research in Computer Security (Esorics)*.

2022 **PC member**, *Formal Foundations and Security of Programmable network Infrastructures (FFSPIN)*, co-located with ACM SIGCOMM.

2022 **PC member**, *IMC (Shadow PC)*.

2020 **Reviewer**, *IEEE Acess Journal*.