Devashish Gosain

✉ *dgosain@mpi-inf.mpg.de*

Current Employment

2022–2023 **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 (CSE)**, *IIIT-Delhi*, India.

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

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

Research Interests

Networks, Privacy, Anonymity, Internet measurements.

Selected Publications

2023 **Thou Shalt Not Reject: Analyzing Accept-Or-Pay Cookie Banners on the Web**, *accepted for publication in proceedings of Internet Measurement Conference (**IMC**)*.
Authors:Ali Rasaii, **Devashish Gosain** and Oliver Gasser

2023 **PTPerf: On the performance evaluation of Tor Pluggable Transports**, *accepted for publication in proceedings of Internet Measurement Conference (**IMC**)*.
Authors: Zeya Umayya, Dhruv Malik, **Devashish Gosain**, Piyush Kumar Sharma

2023 **Poster: Hades: Practical Partitioning Attack on Cryptocurrencies**, *in proceedings of the conference on Network and Distributed System Security (**NDSS**)*.
Authors: Vinay Shetty, Piyush Kumar Sharma, Devashish Gosain

2023 **Cryptographic Deniability: A Multi-perspective Study of User Perceptions and Expectations**, *in proceedings of Usenix Security (**Usenix Security**)*.
Authors: Tarun Kumar Yadav, **Devashish Gosain**, Kent Seamons

2023 **DeeP4R: Deep Packet Inspection in P4 using Packet Recirculation**, *in proceedings of Conference 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**, *in proceedings of Conference on Network and Distributed Security Symposium (**NDSS**)*.
Authors: Piyush Kumar Sharma, **Devashish Gosain**, Claudia Diaz

2023 **Exploring the Cookieverse: A Multi-Perspective Analysis of Web Cookies**, *in proceedings of Conference on Passive and Active Network Measurements (**PAM**)*.
Authors: Ali Rasaii, Shivani Singh, **Devashish Gosain** and Oliver Gasser

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 Award)**, *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

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

Oct. 2019 **CDNs and their role in Internet filtering circumvention**, *Brigham Young University*, Utah, USA.

Feb. 2020 **Internet maps and censorship**, *COSIC, KU Leuven*, Belgium.

June 2023 **Large scale traffic filtering of Android apps**, *TU Delft*, Netherlands.

Services

2023 **PC member**, *Proceedings on Privacy Enhancing Technologies (PoPETS)*.

2023 **PC member**, *European Symposium on Research in Computer Security (Esorics)*.

2023 **PC member**, *International Conference on Applied Cryptography and Network Security (ACNS)*.

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*.

Selected Ongoing Research Projects

The Rise of Accept-Or-Pay Cookie Banners.

Privacy regulations have led to many websites showing cookie banners to their users. Usually, cookie banners present the user with the option to "accept" or "reject" cookies. Recently, a new form of paywall-like cookie banner has taken hold on the Web, giving users the option to either accept cookies (and consequently user tracking) or buy a paid subscription for a tracking-free website experience. In this work, we perform the first completely automated analysis of Cookiewalls, i.e., cookie banners acting as a paywall. We find Cookiewalls on 0.6% of all queried 45k websites. Moreover, Cookiewalls are deployed to a large degree on European websites, e.g., for Germany, we see Cookiewalls on 8.5% of the top 1k websites. Additionally, websites using Cookiewalls send 6.4 times more third-party cookies and 42 times more tracking cookies to visitors compared to regular cookie banner websites. We also uncover two large Subscription Management Platforms used on hundreds of websites, which provide website operators with easy-to-setup Cookiewall solutions.

VoIP Filtering in the Middle East.

There exists a plethora of research on Internet censorship in countries like China and Russia. Similar censorship is also present in many Middle Eastern countries, such as Saudi Arabia, United Arab Emirates, and Iran. The censorship of the Web in these regions is well-known. But, by first-hand reports, some rare news articles, and personal experience, we have been made aware of a novel kind of censorship deployed in the region, focusing exclusively on the voice-over-IP (VoIP) functionalities of many popular messenger applications, e.g., Whatsapp. Thus, for the first time, we are studying the censorship apparatus in the middle east. More specifically, we are conducting measurements to observe what type of VoIP applications are filtered, how many middle eastern countries perform such filtering, and how the censorship infrastructure is technically implemented. Our initial results confirm the presence of sophisticated middleboxes in the region; VoIP calls from WhatsApp, Skype, Discord, etc. are blocked. We are investigating further to pinpoint the location of the middleboxes and ways to circumvent the filtering.

Friend or Foe: Onion Routing and Cryptocurrencies.

In this research, we perform 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 measure the churn and reachability of onion addresses. We found that although onion addresses have high daily churn, they occur relatively more often than IP addresses in longer time frames (e.g., a month). Moreover, we believe 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 confirm the feasibility of the attack in different test scenarios.