

Biographies for the Informational Session on DNS Abuse: Panel Discussion with the ICANN Board

Graeme Bunton



Graeme Bunton is the director of the Domain Name System (DNS) Abuse Institute, an initiative dedicated to developing collaborative and innovative methods of reducing DNS abuse. Graeme has over 11 years of DNS policy experience. Prior to heading the DNS Abuse Institute, he was the head of Policy for TuCows and served as chair of the Registrar Stakeholder Group for four years. Graeme was one of the driving forces behind the 'Framework to Address Abuse,' a new set of guidelines and principles for addressing online harms, which was adopted by more than 50 registries and registrars. He helped found the Citizen Lab at the University of Toronto, and currently serves as board chair of the Internet Infrastructure Coalition.

Stewart Garrick



Stewart Garrick has worked for the Shadowserver Foundation for six years. Previously, he worked 30 years for UK law enforcement (LE), culminating as a senior investigating officer in the National Crime Agency. As a career detective, he worked primarily on major crime units engaged on both proactive and reactive investigations, including many high profile cybercrime cases as the senior investigator, such as the Dridex and Gameover Zeus botnet takedowns. More recently, he has worked in LE supporting roles for Shadowserver. He is currently actively engaged in multiple ongoing international investigations. Mr. Garrick understands the operational challenges, differing evidentiary restrictions, and capabilities across the European Union and worldwide. His focus is always to help LE achieve their intelligence and evidential needs in ways they can actually use. He received a MSc in countering organized crime and terrorism at the University College London (UCL) and a certified information systems security professional (CISSP).

Cristine Hoepers



Dr. Cristine Hoepers holds a degree in computer science and a Ph.D. in applied computing. She is the general manager of CERT.br, maintained by NIC.br, and her work focuses on helping the establishment of new computer security incident response teams (CSIRTs) in the country of Brazil, delivering incident management training, and promoting best practices to increase Internet resilience. In the past Dr. Hoepers served as a member of the Board of Directors for the Forum of Incident Response and Security Teams (FIRST), as a lead expert at the Best Practice Forum on Computer Emergency Response Teams (CERTs) and on Spam in the Internet Governance Forum (IGF) at the United

Nations, and as a member of the International Telecommunication Union High Level Experts Group (ITU HLEG). In 2020 she received from the Malware and Mobile Anti-Abuse Working Group (M³AAWG) the annual Mary Litynski Award for her work to reduce Internet abuse and increase Internet resilience. Dr. Hoepers has also been a speaker and moderator in several forums such as the Anti-Phishing Working Group (APWG), FIRST, ICANN, IGF, the ITU, the Latin America and Caribbean Network Information Centre (LACNIC), M³AAWG, and the Organization of American States (OAS).

Roman Huessy

Roman Huessy is the founder of the non-profit project abuse.ch, which is hosted at the Bern University of Applied Sciences in Switzerland. For over a decade, the project tracks malware and botnets, providing actionable open-source threat intelligence on malicious domain names, IP addresses and websites to the community. Data from abuse.ch is integrated into many commercial and open-source security products. Security software vendors rely on it to protect their customers and many organizations. Internet service providers, and law enforcement and government agencies use it to fight cyber threats that target their constituencies.

Maciej Korczyński



Dr. Maciej Korczyński is an associate professor of computer networks and cybersecurity at the Grenoble Institute of Technology (France). Previously, he was a postdoctoral researcher at TU Delft (Netherlands), analyzing large-scale Internet measurement and incident data to identify how providers of Internet services deal with security risks and incidents. He was also a post-doctoral researcher at Rutgers University (USA), investigating algorithms in distributed anomaly detection systems. He received his Ph.D. in computer science from Grenoble Alps University in 2012.

His main interests revolve around large-scale passive and active measurements for cybersecurity, with a focus on the Domain Name System (DNS). Since 2015, he has co-authored over 30 research papers about domain name abuse, DNS vulnerabilities, DNS reputation metrics, economic incentives for improving the security of the DNS ecosystem, IP spoofing, DDoS attacks, botnets, and vulnerability notifications. The research results were published in selective international research conferences such as the AMC Conference on Computer and Communications Security (ACM CCS), the Network and Distributed System Security Symposium

(NDSS), the ACM Internet Measurement Conference (ACM IMC), the Institute of Electrical and Electronics Engineers European Symposium on Security and Privacy (IEEE Euro S&P), and INFOCOM. Maciej is a member of the Passive DNS Hunters Group, the Domains and Jurisdiction Program Contact Group, Anti-Phishing Working Group (APWG), an academic member of the Messaging, Malware and Mobile Anti-Abuse Working Group (M³AAWG), a research partner for the DNS Abuse Institute Advisory Council, and a designated representative of Grenoble Alps University at Operations, Analysis, and Research Center (DNS-OARC).

Jonathan Matkowsky



Jonathan is a principal researcher at RiskIQ, part of Microsoft Security, Compliance, Identity, and Management. He holds a certified information systems security professional (CISSP) certification, is recognized as a fellow of information privacy by the International Association of Privacy Professionals (IAPP) and is certified by the Global Information Assurance Certification (GIAC) in the laws of data security and investigations. He is AV Preeminent® Martindale-Hubbell® Peer-Rated for the highest standards of professional excellence as an attorney and counselor before the New York Supreme Court and lawyer before the Washington State Supreme Court. He is also currently a research contributor for the Anti-Phishing Working Group (APWG) quarterly trends reports, and a co-chair of the DNS Abuse Special Interest Group within the Forum of Incident Response and Security Teams (FIRST).

Jonathan has published on active defense in the SANS Reading Room, sits on the GIAC Advisory Board, and has appeared over the last 15 years as an expert delegate on Internet fraud, including before the Council of Europe and the Rivest, Shamir, and Adleman (RSA) Conference.