ITC 2023 Alexandria Keynote Talk

Where are the weak keys: RSA keys sharing across PKI ecosystem

Natalia Stakhanova
Director, The CyberLab,
Department of Computer Science,
University of Saskatchewan, Canada
E-mail: nstakhanova@gmail.com, Web: https://www.nataliastakhanova.com/

ABSTRACT

For more than a decade, security researchers have been focusing on the sorry state of public-key infrastructure on the internet, highlighting the widespread prevalence of broken, weak, and vulnerable cryptographic keys. The existence of such keys has significant security implications, including the fact that weaknesses in the keys allow for quicker factorization, enabling one to compute the corresponding private keys more efficiently and undermining communication security. Misconfigurations in cryptographic algorithms and software library implementation decisions can result in identifiable patterns in generated keys, revealing information about the key's origin, such as the originating library, its specific version, and the operating system used. Finally, inadequate randomness in key generation can result in the same key being used for multiple hosts. In this talk, I will explore RSA public key reuse within the PKI ecosystem and its implications.

BIO

Dr. Natalia Stakhanova is the Canada Research Chair in Security and Privacy. Associate Professor at the University of Saskatchewan, Canada. She is a former NB Innovation Research Chair in Cybersecurity at the University of New Brunswick. Her work revolves around building secure systems. Dr. Stakhanova has published over 60 publications in the areas of network security, software protection, and code attribution. She holds 4 patents in the field of computer security. Dr. Stakhanova is a member of the Canadian Cross-Cultural Roundtable on Security (CCRS), the group that provides advice to the Minister of Public Safety Canada and the Minister of Justice and Attorney General of Canada concerning matters of national security and public safety. She serves as an Associate Editor for IEEE Transactions on Dependable and Secure Computing (TDSC), and Guest Editor for IEEE Transactions on Network and Service Management (IEEE TNSM). Dr. Stakhanova is the recipient of numerous recognitions and awards, including the Top 20 Women in Cybersecurity, the CyberNB Recognition Award, the McCain Young Scholar Award, and the Anita Borg Institute Faculty Award. She is a strong advocate of Women in IT and co-founder of CyberLaunch Academy, an initiative that aims to promote science and technology among children.